mbNET®

HANDBUCH

Copyright © MB Connect Line GmbH 2008

Jegliche Vervielfältigung dieses Dokuments, die Verwertung und Mitteilung Ihres Inhalts ist ohne unsere Zustimmung nicht gestattet. Zuwiderhandlungen verpflichten zu Schadenersatz. Alle Rechte vorbehalten.

Diese Bedienungsanleitung beschreibt die Funktionen und Handhabung der Router mbNET

Wir haben versucht die Geräte und Funktionen so gut wie möglich zu beschreiben. Trotz aller Bemühungen können wir für die Richtigkeit des Inhalts keine Gewähr übernehmen. Die neuesten Informationen erhalten Sie auf unseren Internetseiten. Für Verbesserungsvorschläge oder Anregungen sind wir jederzeit dankbar.

Waren- und Firmenzeichen
Die Verwendung eines hier nicht aufgeführten Waren- oder Firmenzeichens ist kein Hinweis auf die freie Verwendbarkeit desselben.

Herausgeber:
MB connect line Fernwartungssysteme GmbH
Raiffeisenstraße 4
74360 Ilsfeld, Deutschland

Telefon: 0049(0)7062/9178788
Fax: 0049(0)7062/9178792
Technische Unterstützung: 0049(0)9851/55776
E-Mail: info@mbconnectline.de
Internet: www.mbconnectline.de

Inhaltsverzeichnis

1. Allgemeines 8
1.1 Kurzbeschreibung 8
1.2 Leistungsmerkmale 8
2. Sicherheitshinweise 9
3. Technische Daten 10
4. Lieferumfang 11
5. Anzeige-, Bedienelemente und Anschlüsse 12
5.1 Ansicht Gerätefrontseite 12
5.2 Ansichten Geräteoberseite, Geräteunterseite und Geräterückseite 14
6. Schnittstellen 15
6.1 Belegung 15
6.1.1 Anschlussbelegung Klemmleiste X1 und X2 auf der Oberseite 15
6.1.2 Anschlussbelegung der RJ12-Buchse auf der Unterseite 15
6.1.3 Anschlussbelegung der seriellen Schnittstellen COM1 und COM2 an der Frontseite 15
6.1.4 Anschlussbelegung LAN- bzw. WAN-Anschluss an der Frontseite 16
6.1.5 Anschlussbelegung USB-Anschluss an der Frontseite 16
7. Inbetriebnahme des Routers 17
7.1 Router an die Versorgungsspannung anschließen und einschalten 17
7.1.1 Router mit Konfigurations-PC verbinden 18
7.2 Voraussetzungen für die Konfiguration 19
7.2.1 Rechneradresse (IP-Adresse) und Netzmaske einstellen 20
7.3 Erste Konfiguration 21
8. Grundkonfiguration des Routers über die Weboberfläche 22
8.1 Die Startseite der Weboberfläche 22
8.2 Beschreibung der Symbole, Schaltflächen und Felder 23
8.3 Systemeinstellungen 24
8.4 Sicherheitseinstellungen 26
8.4.1 Einstellungen speichern 27
9. Beschreibung verschiedener Verbindungsszenarien 28
9.1 Allgemeines 28
9.2 Konfiguration des Industrierouters für eine Verbindung über das Telefonnetz 30
9.2.1 Anschluss und Konfiguration des Routers 31
9.2.1.1 Anschluss des Routers 31
9.2.1.2 Konfiguration des Routers über die Weboberfläche 32
9.2.2 Konfiguration eines Clients (PCs) für den Zugriff auf den Router 37
9.2.3 Verbindung vom Client-PC zum Industrierouter aufbauen 39
9.2.4 Anzeigen und Überprüfen des Verbindungsstatus 39
9.3 Konfiguration des Industrierouters für eine Verbindung mit dem Internet 40
9.3.1 Anschluss und Konfiguration des Routers 41
9.3.1.1 Anschluss des Routers 41
9.3.1.2 Konfiguration des Routers über die Weboberfläche 42
9.3.2 Einwahl Router ins Internet 47
9.3.3 Anzeigen der Internetverbindung 47

9.4 Konfiguration des Industrierouters unter Einsatz eines DSL-Modem für eine Verbindung mit dem Internet 48
9.4.1 Anschluss und Konfiguration des Routers 49
9.4.1.1 Anschluss des Routers 49
9.4.1.2 Konfiguration des Routers über die Weboberfläche 50
9.4.2 Verbindung zwischen Client-PC und Router herstellen 53
9.4.3 Anzeigen des Verbindungsstatus 54

9.5 Konfiguration des Industrierouters bei bereits bestehendem Router für eine Verbindung ins Internet 55
9.5.1 Anschluss und Konfiguration des Routers 56
9.5.1.1 Anschluss des Routers 56
9.5.1.2 Konfiguration des Routers über die Weboberfläche 57

9.6 Konfiguration des Industrierouters für eine VPN-Verbindung mit einem Client 60
9.6.1 Anschluss und Konfiguration des Routers 61
9.6.1.1 Anschluss des Routers 61
9.6.1.2 Benutzer für VPN-Einwahl anlegen 61
9.6.1.3 Konfiguration des Routers (VPN-Server) 62
9.6.2 Konfiguration eines Client-PCs für eine VPN-Verbindung zum Router 66
9.6.3 Verbindung zwischen Client-PC und Router über VPN aufbauen 68
9.6.3.1 Einwahl Router ins Internet 68
9.6.3.2 Aufbau einer VPN-Verbindung des Clients zum Router 68
9.6.3.3 Weitere Einstellungen 68

9.7 Konfiguration der Verbindung zwischen zwei Industrieroutern per VPN-PPTP 69
9.7.1 Einstellungen für eine Verbindung zwischen zwei Industrieroutern - PPTP-Server 70
9.7.2 Einstellungen für eine Verbindung zwischen zwei Industrieroutern - PPTP-Client 72

10. Zertifikate und Widerrufslisten erstellen mit XCA 75

10.1 Überblick Zertifikate 75

10.2 Erstellen von Zertifikaten 76
10.2.1 Erstellung eines Stammzellenzertifikats 76
10.2.1.1 Stammzertifikat Herkunft 77
10.2.1.2 Stammzertifikat Besitzer 78
10.2.1.3 Stammzertifikat Extensions 79
10.2.1.4 Stammzertifikat Key Usage 81
10.2.2 Erstellung eines Clientzertifikats 83
10.2.2.1 Clientzertifikat - Herkunft 83
10.2.2.2 Clientzertifikat - Besitzer 85
10.2.2.3 Clientzertifikat - Extensions 86
10.2.2.4 Clientzertifikat - Key Usage 87
10.2.2.5 Clientzertifikat - Netscape 87

10.3 Erstellen von CRL-Dateien (Widerrufslisten) 90

11. Zertifikate unter Windows XP importieren 92

12. Systemeinstellungen 94

12.1 System – WEB 95

12.2 System – Benutzer 96
12.2.1 Allgemeines 96
12.2.2 Benutzer editieren 96
12.2.3 Benutzer anlegen 97
12.2.4 Benutzer löschen 98

12.3 System - Zertifikate 99
12.3.1 Eigene Zertifikate 100
12.3.2 CA 102
12.3.3 Partner Zertifikate 103
12.3.4 CRL 104

12.4 System - USB 105

12.5 System - Protokollierung 106
12.6 System - Konfiguration 107
12.7 System - Firmware 108
13. Netzwerk 110
13.1 Netzwerk - LAN 110
13.2 Netzwerk - WAN 111
13.3 Netzwerk - Modem 113
13.3.1 Netzwerk-Modem-Eingehend 113
13.3.2 Netzwerk-Modem-Ausgehend 115
13.3.3 Netzwerk – Modem-Rückruf 116
13.3.4 Netzwerk-Modem-SMS 117
13.4 Netzwerk - Internet 118
13.5 Netzwerk - DHCP 120
13.6 Netzwerk - DNS-Server 121
13.7 Netzwerk - Hosts 122
13.8 Netzwerk - DynDNS 123
13.8.1 Allgemeines 123
13.8.2 Vorgehensweise zur Einrichtung der DynDNS-Konfiguration 123
14. Serielle Schnittstellen 126
14.1 Allgemeines 126
14.2 Serielle Schnittstellen auf Ihrem PC umleiten (VCOM LAN2) 129
14.2.1 Einstellungen zu Simatic Manager 129
15. Sicherheitseinstellungen 130
15.1 Allgemeines 130
15.2 WAN>LAN 131
15.3 LAN>WAN 132
15.4 Forwarding 133
15.5 NAT 134
16. VPN - IPSec 135
16.1 Beschreibung zur Konfiguration einer VPN-IPSec Verbindung mit zwei Routern 135
16.1.1 Verbindungseinstellungen 136
16.1.2 Netzwerkeinstellungen 137
16.1.3 Authentisierung 137
16.1.4 Protokolleinstellungen 141
16.1.5 L2TP Server Konfiguration 142
17. VPN - PPTP 143
17.1 Servereinstellungen 143
17.2 Clienteinstellung 145
18. VPN - OpenVPN 146
18.1 Grundsätzliches zu OpenVPN 146
18.2 Verbindungsszenarien 147
18.2.1 Client – Router 147
18.2.1.1 Keine Authentisierung oder statischer Schlüssel 149
18.2.1.2 Authentisierung mit Zertifikaten 149
18.2.1.3 OpenVPN Windowsclient konfigurieren 150

18.2.1.3.1 Keine Authentifizierung ... 151
18.2.1.3.2 Authentifizierung eines Windowsclient mit statischem Schlüssel ... 152
18.2.1.3.3 Starten der OpenVPN-Verbindung ... 153
18.2.2 Router-Router ... 153
18.2.2.1 Server – keine Authentifizierung oder statischer Schlüssel ... 155
18.2.2.2 Server – Authentifizierung mit Zertifikaten ... 155
18.2.2.2.1 Single Client: nur ein Client kann sich einwählen ... 156
18.2.2.2.2 Multi Client: mehrere Clients können sich einwählen ... 157
18.2.2.3 Client –Authentifizierung: kein oder statischer Schlüssel ... 158
18.2.2.4 Client – Authentifizierung: mit Zertifikate ... 159
18.2.3 Authentifizierung ... 160
18.2.3.1 Keine Authentifizierung ... 160
18.2.3.2 Authentifizierung mit statischem Schlüssel ... 160
18.2.3.2.1 Schlüsselmanagement ... 161
18.2.3.3 Authentisierung mit Zertifikate ... 162
18.2.3.3.1 Authentifizierung mit CA- und eigenem Zertifikat ... 162
18.2.3.3.2 Authentifizierung mit CA- und eigenem Zertifikat und Benutzer/Passwort ... 164
18.2.3.3.3 Server ... 164
18.2.3.3.4 Client ... 165
18.3 Inaktivitätseinstellungen ... 167
18.4 Protokolleinstellungen ... 168
19. Alarmmanagement ... 170
19.1 Allgemeines ... 170
19.2 Digitale Eingänge ... 170
19.3 Digitale Ausgänge ... 172
20. Statusmeldungen ... 173
20.1 Allgemeines ... 173
20.2 Status - Schnittstellen ... 173
20.3 Status - Netzwerk ... 174
20.4 Status - Modem ... 175
20.5 Status - Internet ... 177
20.6 Status - DHCP ... 179
20.7 Status - DNS-Server ... 180
20.8 Status - DynDNS ... 181
20.9 Status - NTP ... 182
20.10 Status - VPN-IPSEC ... 183
20.11 Status - VPN-PPTP ... 184
20.12 Status – VPN OpenVPN ... 185
20.13 Status - Diagnose ... 186
20.14 Status - USB ... 187
20.15 Status - Alarmmanagement ... 188
20.16 Status - System ... 189
21. Werksseitige Einstellung bei Auslieferung ... 190
21.1 Benutzername und Passwort ... 190
21.2 IP-Adresse des Routers ... 190
22. Werkseinstellung laden ... 190

23. Modeminitialisierung 191
Allgemeine Hinweise zu den AT-Befehlen 191
23.1 Befehle des Analog-Modems 191
23.2 Befehle des ISDN Terminal Adapters (TA) 193
24. Anhang 194
24.1 Ländercodes für analoge Geräte 194
25. Index 199

1. Allgemeines

1.1 Kurzbeschreibung

Der Industrierouter *mbNET* bietet Ihnen höchste Flexibilität bei größtmöglicher Sicherheit. Mit dem Router können Sie eine einfache und sichere Kommunikation von der Ferne aus mit Ihren Anlagen herstellen. Durch die kompakte Bauform findet der Router *mbNET* in jedem Schaltschrank Platz und bietet durch seine Vielzahl an Schnittstellen und Gerätetreibern das perfekte System zur Anbindung an die verschiedensten Steuerungssysteme. Über die Weboberfläche lässt sich der Router *mbNET* konfigurieren.

1.2 Leistungsmerkmale

- Vollständige Konfiguration des Routers über Weboberfläche durch lokal angeschlossenen PC oder von der Ferne aus.
- Weltweit einsatzfähig durch verschiedene Modemanschaltungen (ISDN, Analog) und Zugriff über LAN und Internet.
- Herstellung sicherer Verbindungen durch integrierten Firewall mit IP-Filter, NAT und Port-Forwarding und VPN mit Verschlüsselungsverfahren AES, DES/3DES und Authentisierung mittels Pre-Shared-Key oder X.509 Zeritifkate.
- Alarmmanagement:
  - mit Hilfe von frei konfigurierbaren digitale Ein- und Ausgängen und Versand durch Email und Einwahl ins Internet.
  - durch Fernschalten von Ausgängen beim Auftreten von Störungen oder bei aktiver Internetverbindung.
- Integrierter Server zum Sichern sämtlicher Einstellungen und zur Freigabe von Daten im Netzwerk über angeschlossenen USB-Stick oder USB-Festplatte.
- Konfigurierbare RS-Schnittstelle RS232,RS485,RS422 oder optional MPI/Profibus zum Anschluss von Steuerungssystemen.

2. Sicherheitshinweise

- Der Router ist nach dem Stand der Technik und den anerkannten sicherheitstechnischen Regeln gebaut (siehe Konformitätserklärung).

- Der Router muss an einem trockenen Platz montiert werden. Es dürfen keine Flüssigkeiten in das Innere des Routers eindringen, da hierbei elektrische Schläge oder Kurzschlüsse die Folge sein könnten.

- Der Router ist nur für die Anwendung innerhalb von Gebäuden und nicht im Freien vorgesehen.

- Öffnen Sie niemals das Gehäuse des Routers. Durch unbefugtes Öffnen und unsachgemäße Reparatur können Gefahren für die Benutzer des Routers entstehen. Der Hersteller übernimmt für eigenmächtige Veränderungen keinerlei Gewährleistung.
  Die Garantie erlischt mit dem Öffnen des Gerätes!

- Der Router darf gemäß europäischen Vorgaben und deutschem Elektronik und Elektronikgerätegesetz nicht über den normalen Hausmüll entsorgt werden. Das Gerät ist entsprechend zu entsorgen.

3. Technische Daten

Spannung V (DC)	10 – 30V
Stromaufnahme	max. 300mA bei 24V
Digitale Eingänge	4 digitale Eingänge (10-30V) (abgesichert)
Digitale Ausgänge	2 digitale Ausgänge (200mA max. / Ausgang)
Schutzklasse IP	20
Einsatzbereich	Trockene Umgebung
Temperatur (Betrieb)	0...50°C
Temperatur (Lager)	-20...+60°C
Gewicht	Ca. 500 g
Luftfeuchtigkeit	0...95% nicht kondensierend
Abmessungen (max.)	B x H x T: 57 x 106 x 145
Schnittstellen	Geräteabhängig RS232/485, RS422, MPI/Profibus, LAN 10/100 MBit/s
Allgemeine Zulassung	EN 61000-6-4:2001, Störaussendung für Industriebetriebe EN 61000-6-2:2001, Störfestigkeit für Industriebetriebe

4. Lieferumfang

Überprüfen Sie zuerst, ob in der Produktpackung folgende Teile enthalten sind:

- ❑ **Router *mbNET***

Abbildung 1: Router *mbNET*

- ❑ **Netzwerkkabel (Belegung 1 zu 1)**
- ❑ **1 Netzwerkkabel gekreuzt (Crossover)**

Abbildung 2: Netzwerkkabel Belegung 1 zu 1

Abbildung 3: Netzwerkkabel gekreuzt

- ❑ **Bei den Routervarianten mit Analog-Modem: Kabel mit RJ10-Stecker und Adapter von RJ10- auf TAE-Stecker**
- ❑ **Bei den Routervarianten mit ISDN-Modem: Kabel mit RJ10- und RJ45-Stecker**

Abbildung 4: Kabel für Analoganschluss

Abbildung 5: Kabel für ISDN-Anschluss

- ❑ **Kurzanleitung**

Abbildung 6: Kurzanleitung

Sollte eines dieser Teile fehlen oder beschädigt sein, wenden Sie sich bitte an die folgende Firma:

MB CONNECT LINE GMBH
Winnettener Straße 5
D-91550 Dinkelsbühl
Tel.: +49(0)9851/55776
Fax: +49(0)9851/55882
E-Mail: info@mbconnectline.de
Internet: www.mbconnectline.de

Bewahren Sie den Karton sowie das Original-Verpackungsmaterial für den Fall auf, dass Sie das Gerät zu einem späteren Zeitpunkt zur Reparatur einsenden müssen.

5. Anzeige-, Bedienelemente und Anschlüsse

5.1 Ansicht Gerätefrontseite

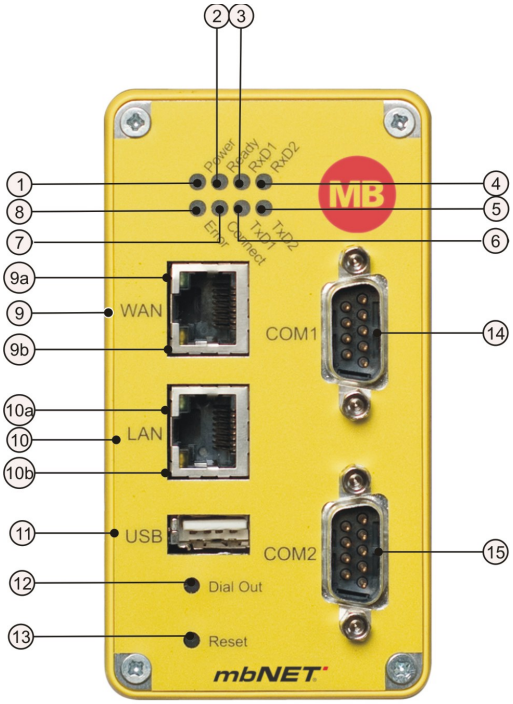


Abbildung 7: Ansicht Gerätefront

Pos.	Bezeichnung	Status	Beschreibung
1	Power	LED aus	Stromversorgung für Router ist ausgeschaltet bzw. Router ist nicht an die Stromversorgung / Netzteil angeschlossen.
		LED ein	Stromversorgung ist an der Klemmleiste angeschlossen und eingeschaltet.
2	Ready	LED blinkt	Nach dem Einschalten ist die Ready-LED für ca. 10 Sekunden noch aus, während die Power-LED sofort leuchtet. Nach ca. 10 Sekunden blinkt die READY-LED (Starten des Betriebssystems). Nach ca. 40 Sekunden sollte die Ready-LED dann dauerhaft leuchten.
		LED Dauerlicht	
3	RxD1	LED aus	Keine Empfangsdaten an der seriellen Schnittstelle COM1.
		LED ein	Datenempfang an der seriellen Schnittstelle COM1.
4	RxD2	LED aus	Keine Empfangsdaten an der seriellen Schnittstelle COM2.
		LED blinkt	Datenempfang an der seriellen Schnittstelle COM2.
5	TxD2	LED aus	Keine Datensendung an der seriellen Schnittstelle COM2.
		LED blinkt	Datensendung an der seriellen Schnittstelle COM2.
5	TxD1	LED aus	Keine Datensendung an der seriellen Schnittstelle COM1.
		LED blinkt	Datensendung an der seriellen Schnittstelle COM1.
7	Connect	LED aus	Router ist nicht mit dem Internet verbunden.
		LED ein	Router ist mit dem Internet verbunden. Leuchtet nicht, bei einer Wählverbindung.
		LED blinkt	VPN-Verbindung aktiv (ab Firmware V1.3.0)
8	Error	LED aus	Router arbeitet fehlerfrei.
		LED ein	Am Router ist ein Fehler aufgetreten. Diagnose unter Status-System (siehe **Status - System**)

Bedienelemente, Anschlüsse und Anzeigeelemente

Ansicht Gerätefrontseite

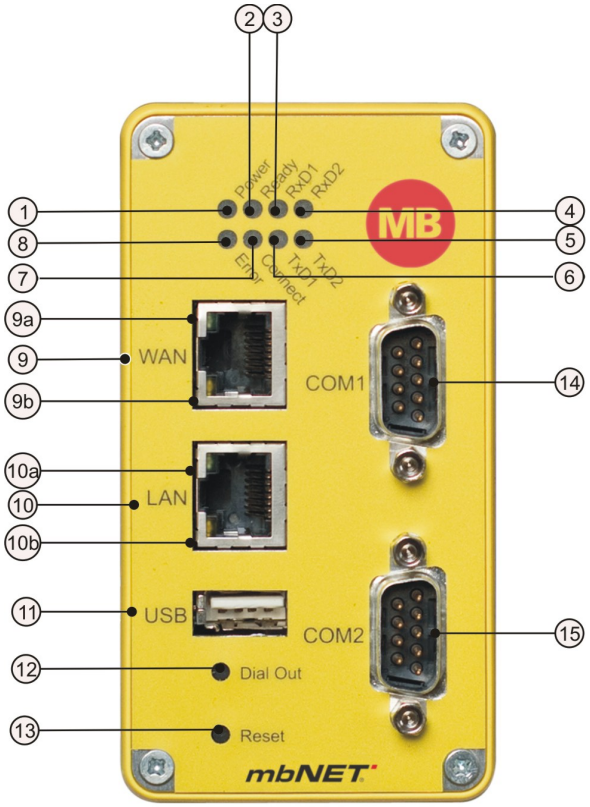


Abbildung 8: Ansicht Gerätefront

Pos.	Bezeichnung	Status	Beschreibung
9	**WAN**	-	WAN-Anschluss des Routers.
9a	**WAN-LED**	LED grün leuchtet auf	Netzwerkverbindung vorhanden.
9b	**WAN-LED**	LED orange blinkt	Netzwerkdatenverkehr aktiv.
10	**LAN**		Anschluss des lokalen Netzwerkes (z.B. Maschinennetz).
10a	**LAN-LED**	LED grün leuchtet auf	Netzwerkverbindung vorhanden.
10b	**LAN-LED**	LED orange blinkt	Netzwerkdatenverkehr aktiv
11	**USB**	-	Anschluss für USB-Stick.
12	**Dial out**	-	Diese Taste dient zum Aufbau einer Internetverbindung.
13	**Reset**	-	Nach Betätigen der Taste wird der Router neu gestartet (sog. Kaltstart).
14	**COM1**		Schnittstelle COM1 zur Anbindung von Geräten mit RS232 / RS485, RS422-Schnittstelle.
15	**COM2**	-	Schnittstelle COM2 zur Anbindung von Geräten mit MPI-Schnittstelle.

Bedienelemente, Anschlüsse und Anzeigeelemente

5.2 Ansichten Geräteoberseite, Geräteunterseite und Geräterückseite

Ansicht Geräteoberseite **Ansicht Geräteunterseite** **Ansicht Geräterückseite**

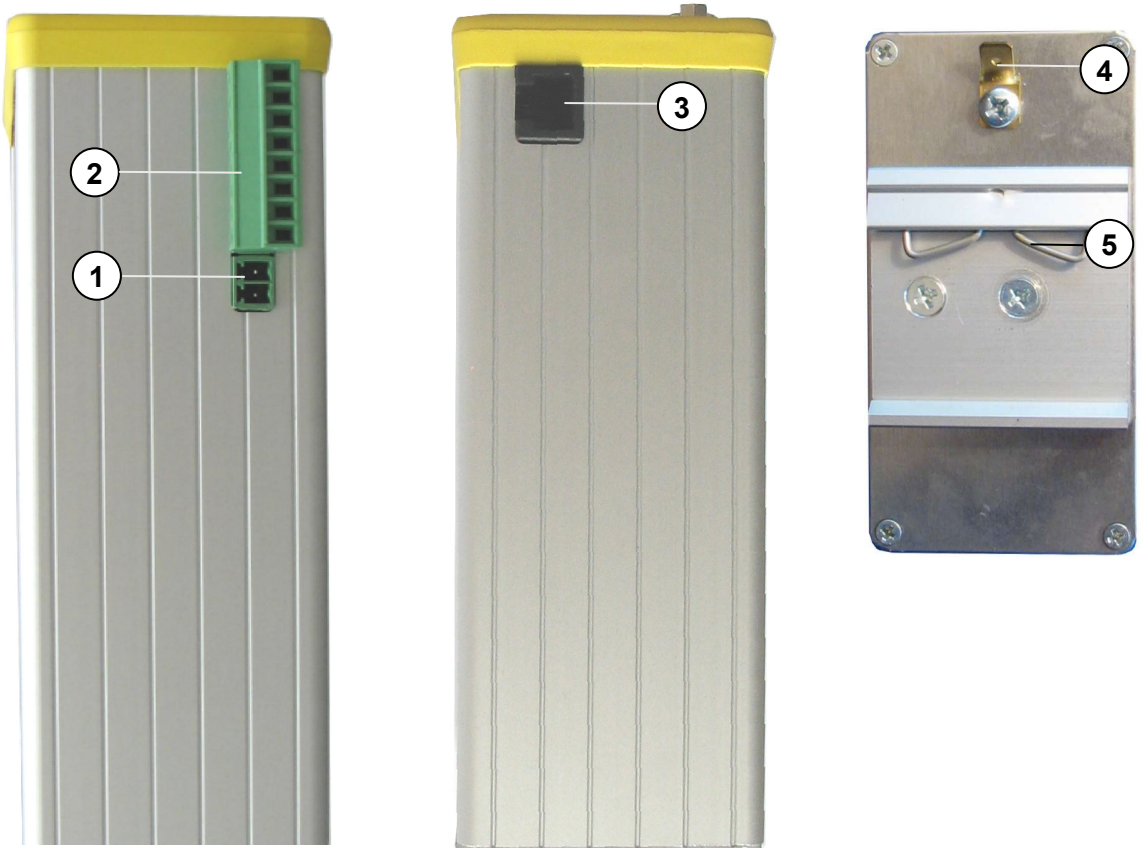


Abbildung 9: Ansicht Geräteober- und Geräteunterseite

Die obige Abbildung zeigt die interne Verschaltung und den Anschluss der Ein- und Ausgänge. Die Anschlussbelegung der Klemmleiste entnehmen Sie bitte der Tabelle auf der nachfolgenden Seite.

Pos.	Beschreibung
1	Klemmleiste X1 zum Anschluss der Versorgungsspannung
2	Klemmleiste X2 zum Anschluss der digitalen Eingänge und Ausgänge
3	RJ-12-Buchse zum Anschluss des im Router integrierten Analog- bzw. ISDN-Modems
4	Erdungsfahne zum Anschluss des Potentialausgleichs
5	Feder zum Einrasten in Hutschiene

6. Schnittstellen

6.1 Belegung

6.1.1 Anschlussbelegung Klemmleiste X1 und X2 auf der Oberseite

X1	**+**	Anschluss Versorgungsspannung 10-30V DC
	-	Anschluss 0V DC
X2	**1**	Digitaler Eingang E1 (10-30V DC)
	2	Digitaler Eingang E2 (10-30V DC)
	3	Digitaler Eingang E3 (10-30V DC)
	4	Digitaler Eingang E4 (10-30V DC)
	P	Abgesicherte Spannung 10-30V DC
	M	Anschluss 0V DC
	02	Digitaler Ausgang A2
	01	Digitaler Ausgang A1

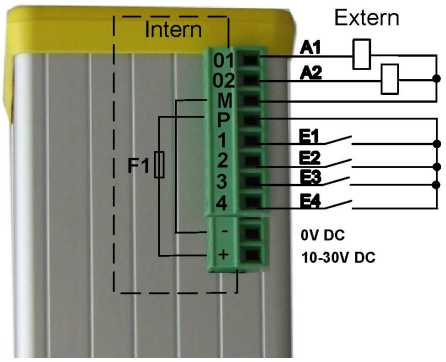


Abbildung 10

6.1.2 Anschlussbelegung der RJ12-Buchse auf der Unterseite

Pin	ISDN	Analog
1	Nicht belegt	Nicht belegt
2	TX+	Nicht belegt
3	RX+	Lb/b
4	RX-	La/a
5	TX-	Nicht belegt
6	Nicht belegt	Nicht belegt

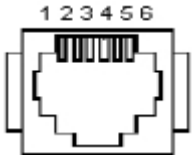


Abbildung 11

6.1.3 Anschlussbelegung der seriellen Schnittstellen COM1 und COM2 an der Frontseite

Pin	RS 232	RS 485	MPI
1	DCD Data Carrier Detect	Nicht belegt	Nicht belegt
2	RxD Receive Data	RxD – Receive Data	GND 24V
3	TxD Transmit	TxD + Transmit Data	Datenleitung B
4	DTR Data Terminal Ready	+5Volt (nur bei 4-Draht Betrieb)	Sendeanforderung
5	Signal Ground	Signal Ground	GND 5V(200mA)
6	DSR Data Set Ready	nicht belegt	5V Ausgang
7	RTS Request To Send	TxD – Transmit Data	24V Versorgungs-eingang
8	CTS Clear to Send	RxD+ Receive Data	Datenleitung A
9	RI Ring Indicator	Nicht belegt	Sendeanforderung

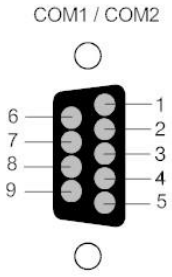


Abbildung 12

6.1.4 Anschlussbelegung LAN- bzw. WAN-Anschluss an der Frontseite

	Signal
1	TX+
2	TX-
3	RX+
4	Nicht belegt
5	Nicht belegt
6	RX-

Abbildung 13

6.1.5 Anschlussbelegung USB-Anschluss an der Frontseite

	Signal
1	VCC (+5V)
2	- Data
3	+Data
4	GND

Abbildung 14

7. Inbetriebnahme des Routers

7.1 Router an die Versorgungsspannung anschließen und einschalten

Der Router ist für den Schaltschrankeinbau vorgesehen. Das Gerät ist konzipiert für die Montage auf Hutschienen (gemäß DIN EN 50 022).

Bitte beachten Sie!
Vor der Verbindung des Routers mit einem Netzwerk oder mit einem PC muss der Router zuerst ordnungsgemäß an die Versorgungsspannung angeschlossen werden, da sonst evtl. weitere Geräte zerstört werden können. Gehen Sie deshalb wie nachfolgend beschrieben vor!

ACHTUNG!
Potentialausgleich an der Erdungslasche auf der Rückseite des Routers anschließen!

Abbildung 15: Anschluss Potentialausgleich

- ❑ Router in die DIN-Hutschiene einrasten lassen. Dazu die obere Führung an der Hutschiene ansetzen und den Router danach nach unten gegen die Hutschiene drücken bis er vollständig einrastet.

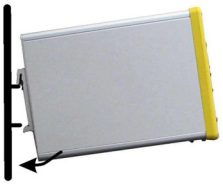


Abbildung 16: Router mit Hutschiene

- ❑ Schließen Sie die Versorgungsspannung (10-30V DC) an die **Klemme X1** des Routers an.

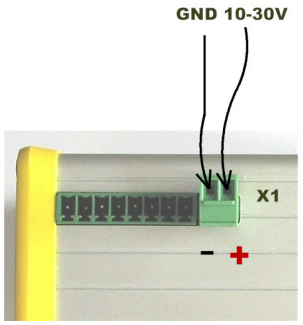


Abbildung 17: Anschlussklemmen X1 für Versorgungsspannung

Auf richtige Polung achten!

- ❑ Schalten Sie jetzt die Versorgungsspannung ein. Es muss sofort die grüne Leuchtdiode **Power** aufleuchten. Nach ca. 40s sollte die Leuchtdiode **Ready** dauerhaft leuchten. Das Gerät ist daraufhin betriebsbereit.

Abbildung 18:
Leuchtdioden Power und Ready

Für weitere Unterstützung rund um den Industrierouter mbNET besuchen Sie uns auf unserer Homepage www.mbconnectline.de im Support-Forum

Inbetriebnahme des Routers (Fortsetzung)

7.1.1 Router mit Konfigurations-PC verbinden

- ❑ Bevor Sie den Router konfigurieren, müssen Sie ihn über das beigefügte Netzwerkkabel (**1**) (Crossover-Kabel) mit dem Rechner verbinden. Stecken Sie hierzu das eine Ende des Netzwerkkabels in den **LAN-Anschluss** des Routers und das andere Ende in die Netzwerkkarte des Rechners.

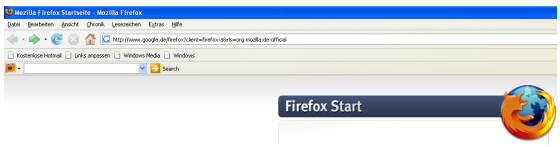
Abbildung 19

Inbetriebnahme des Routers (Fortsetzung)

7.2 Voraussetzungen für die Konfiguration

Voraussetzungen für die Konfiguration des Routers sind:

- ❑ **ein PC mit Netzwerkkarte**



- ❑ **ein Internetbrowser** (z.B. Firefox oder Internet Explorer)

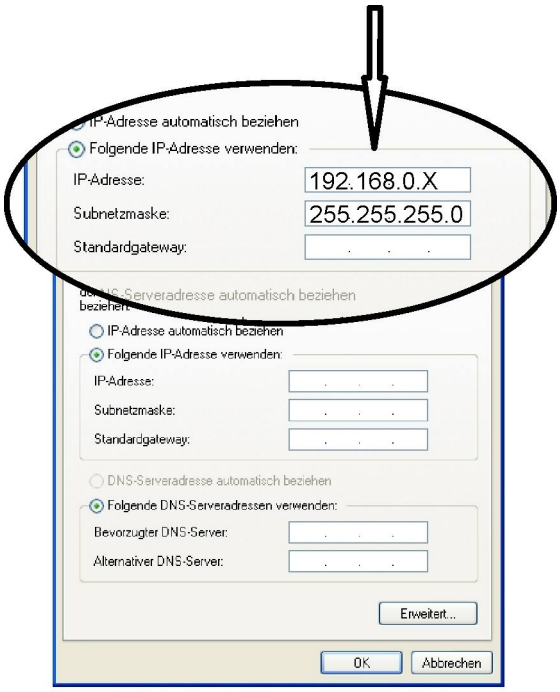


Abbildung 20

- ❑ **Folgende Einstellungen müssen Sie an Ihrem PC durchführen:**
  - **Die IP-Adresse des Rechners muss so eingestellt werden, dass sie im Netz 192.168.0.X liegt**
    X: variabel
  - **die Netzmaske muss 255.255.255.0 lauten**

Die Vorgehensweise, wie Sie die erforderlichen Einstellungen an einem PC durchführen, entnehmen Sie bitte der folgenden Seite.
Falls Ihnen die Vorgehensweise zur Einstellung der IP-Adresse und der Netzmaske bereits bekannt ist, stellen Sie diese wie oben beschrieben entsprechend ein und fahren Sie fort mit der Konfiguration in Kapitel **Erste Konfiguration**

Inbetriebnahme des Routers (Fortsetzung)

7.2.1 Rechneradresse (IP-Adresse) und Netzmaske einstellen

Zum Einstellen der IP-Adresse gehen Sie bitte folgendermaßen vor:

- ❑ Wechseln Sie zunächst in Windows in die Systemsteuerung (**1**) und doppelklicken Sie dann auf Netzwerkverbindungen (**2**).
- ❑ Klicken Sie mit der rechten Maustaste auf **LAN-Verbindung (3)** und wählen Sie die Option **Eigenschaften.**
- ❑ In dem folgenden Fenster doppelklicken Sie die Option **Netzwerkprotokoll (TCP/IP) (4).**
- ❑ In dem neuen Fenster geben Sie die entsprechende IP-Adresse ein. Es bietet sich z.B. die IP-Adresse **192.168.0.2** an.

Bitte beachten Sie!
Die IP-Adresse muss im Netz 192.168.0.X liegen.

- ❑ Als Subnetzmaske geben Sie **255.255.255.0** und als Standardgateway die unter Kapitel **IP-Adresse des Routers** aufgeführte IP-Adresse des Routers.
- ❑ Bei DNS-Server bietet sich an die Option „**DNS-Serveradresse automatisch beziehen**“ auszuwählen.
- ❑ Zum Abschließen und Speichern der Einstellungen klicken Sie jeweils auf die Schaltfläche **OK** der geöffneten Fenster.

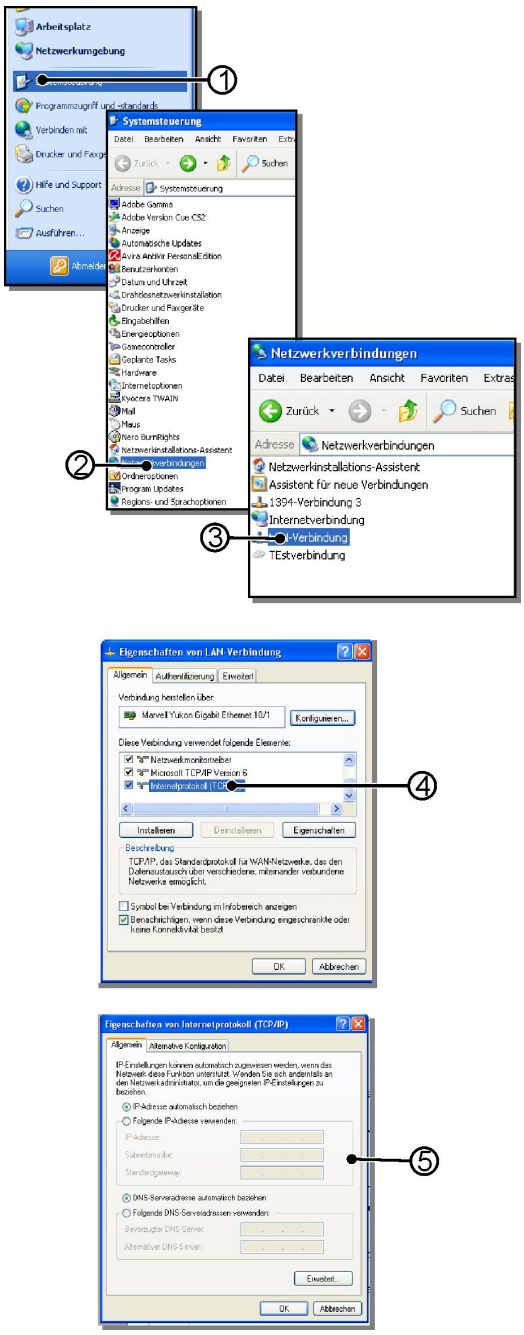


Abbildung 21

Inbetriebnahme des Routers (Fortsetzung)

7.3 Erste Konfiguration

Gehen Sie folgendermaßen vor:
Starten Sie Ihren Browser und geben Sie in der Adresszeile die erforderliche IP-Adresse des Routers ein.

Werkseinstellung ist: 192.168.0.100

Abbildung 22

Melden Sie sich mit folgenden Einstellungen am Router an:

- ☐ Benutzername: admin
- ☐ Passwort: kein Passwort notwendig

Abbildung 23

Firmware kleiner 1.2.0

Nach erfolgreicher Anmeldung wird die **Startseite der Konfigurationsoberfläche** (siehe Abbildung rechts) angezeigt.

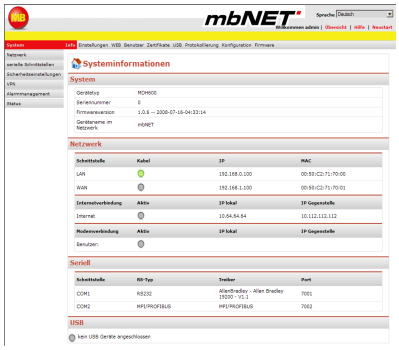


Abbildung 24

Ab **Firmware-Version 1.2.0** ist ein Verbindungsassistent (Wizard) implementiert, der Ihnen das Erstellen von Netzwerk-/, Internet-/ und VPN-Verbindungen erleichtert. Der Assistent leitet Sie Schritt für Schritt durch die Konfigurationsprozesse und funktioniert intuitiv. Sie können den Wizard auch manuell aufrufen. Klicken Sie hierzu rechts oben im Browserfenster auf „Assistenten“.

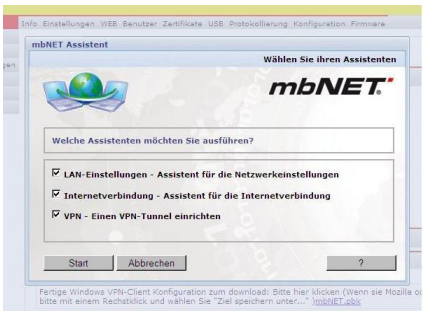


Abbildung 25

8. Grundkonfiguration des Routers über die Weboberfläche

8.1 Die Startseite der Weboberfläche

Die Startseite ist so konzipiert, dass Sie auf einen Blick die wichtigsten Informationen über den Zustand bzw. Zugriff auf den Router *mbNET* erhalten. Die seitliche Navigationsleiste (**1**) und die obere Navigationsleiste (**2**) werden Sie während der Konfiguration des Routers begleiten. Zu jedem der in der seitlichen Navigationsleiste (**1**) aufgeführten Punkte werden die entsprechenden Unterpunkte (**2**) in der oberen Navigationsleiste angezeigt.

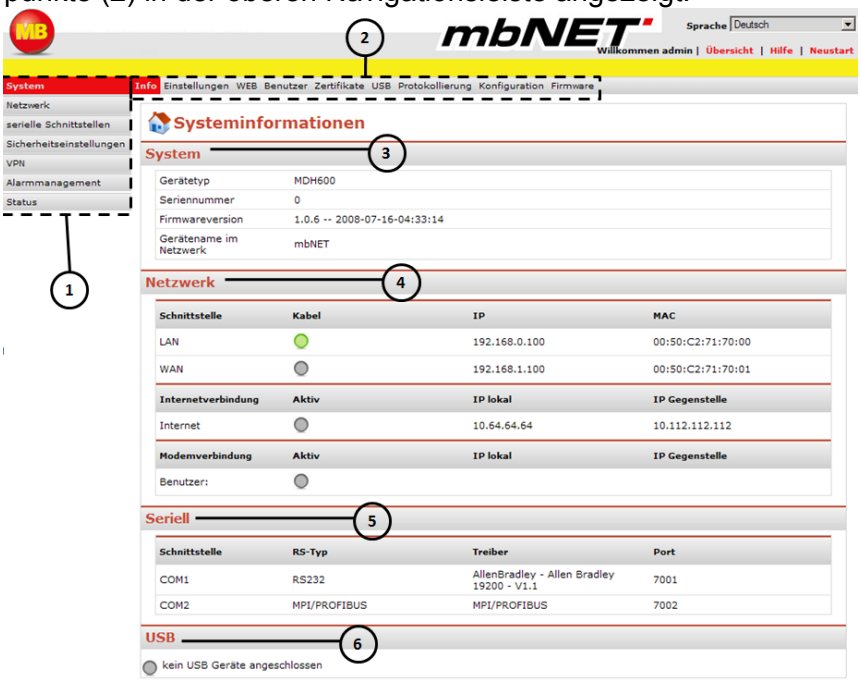
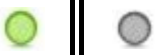


Abbildung 26: Menümaske Systeminformationen

Pos.	Bezeichnung	Funktion
3	**System**	Systeminformationen wie Gerätetyp, Gerätename, aktueller Firmwarestand und Seriennummer des Routers.
4	**Netzwerk**	**Interface: LAN – WAN:** Zeigt an, welche Netzwerkanschlüsse im Augenblick im bestehenden Netzwerk über die entsprechenden Buchsen verbunden / angeschlossen sind. Eine bestehende Verbindung wird durch ein grünes Symbol angezeigt. **Internetverbindung:** Eine momentan aktive Verbindung ins Internet (auch Verbindungen ins Internet) wird durch einen grün ausgefüllten Kreis dargestellt. Besteht dagegen momentan keine aktive Verbindung ins Internet, dann wird dies durch einen grau ausgefüllten Kreis angezeigt. **Modem Verbindung:** Hier werden nur die **eingehenden** Modemverbindungen angezeigt. Falls eine Verbindung mit dem Modem hergestellt wurde, wird dies durch einen grün ausgefüllten Kreis dargestellt. Zugleich wird der Benutzer angezeigt, der mit dem Modem verbunden ist.
5	**Seriell**	Hier wird die aktuelle Konfiguration der Schnittstellen **COM1** und **COM2** angezeigt.
6	**USB**	Information über angeschlossen USB-Speicher. Ein angeschlossener Speicher (z.B. USB-Stick oder extern angeschlossene Festplatte) wird durch einen grün ausgefüllten Kreis dargestellt.

8.2 Beschreibung der Symbole, Schaltflächen und Felder

Im weiteren Verlauf dieser Bedienungsanleitung werden Sie immer wieder auf bestimmte Symbole stoßen, deren Bedeutung auf der folgenden Seite ausführlich beschrieben werden

Nr.	Symbol und Feldertypen	Beschreibung
1		**Grau dargestellte LED:** Verbindung nicht aktiv / Kabel oder USB-Gerät nicht angeschlossen. / **Grün dargestellte LED:** Verbindung aktiv bzw. Kabel oder USB-Gerät angeschlossen.
2		Diese Schaltfläche erscheint immer dort, wo Einstellungen vorgenommen werden können. Sie dient zum temporären Abspeichern der momentanen Konfiguration, d.h. wird der Router neu gestartet, dann sind die geänderten Einstellungen verloren. Zum dauerhaften Abspeichern der Einstellungen ist die Schaltfläche Nr. 5 anzuklicken.
3		Wenn Sie Ihre Eingaben zuvor nur temporär gespeichert haben (siehe Nr. 2), dann können Sie diese hiermit wieder durch Betätigen dieser Schaltfläche zurücksetzen.
5		Hiermit werden alle gespeicherten Änderungen dauerhaft auf dem Router gespeichert und übernommen.
6		Sog. Checkbox. Durch Anklicken des entsprechenden Feldes kann die entsprechende Option aktiviert / deaktiviert werden.
7		In diesem Eingabefeld müssen Sie, falls erforderlich, die Eingaben per Hand durchführen.
8		Durch Anklicken des mit einem Häkchen markierten Kästchens treffen Sie bitte die entsprechende Auswahl (Auswahlfeld).
9		Wenn Sie dieses Feld anklicken, dann können Sie die Einstellungen in der entsprechende Zeile ändern (editieren).
10		Um die in der entsprechenden Zeile durchgeführten Änderungen rückgängig zu machen, klicken Sie bitte auf diese Schaltfläche.
11		Hiermit speichern Sie temporär die in momentan bearbeiteten Einstellungen. Um die Änderungen im Router dauerhaft abzuspeichern, ist die Schaltfläche Nr. 5 anzuklicken.
12		Zeile für weitere Eingaben hinzufügen. Bevor Sie auf diese Schaltfläche klicken, muss die momentan angezeigte Zeile Werte bzw. Angaben enthalten. Ansonsten erfolgt eine Fehlermeldung im oberen Bereich der aktuellen Konfigurationsseite.
13		Hiermit löschen Sie die entsprechenden Eingaben in der momentanen Bearbeitungszeile.
14		Hiermit können Sie die Reihenfolge von Regeln ändern.

Grundkonfiguration des Routers über die Weboberfläche

8.3 Systemeinstellungen

Bevor Sie den Industrierouter *mbNET* speziell für Ihren Anwendungsfall konfigurieren, sollten Sie vorab bestimmte Grundeinstellungen vornehmen.
Gehen Sie hierzu wie nachfolgend beschrieben vor:

- ❑ Klicken Sie auf der Startseite der Weboberfläche in der oberen Navigationsleiste auf die Schaltfläche **System** und **Einstellungen**.
  Es wird daraufhin die nachfolgende Menümaske mit den Systemeinstellungen angezeigt.
  Gehen Sie nun, wie auf den folgenden Seiten beschrieben, entsprechend vor.

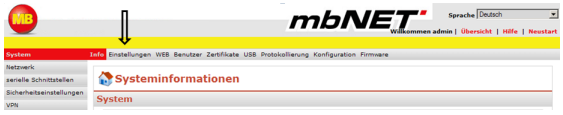


Abbildung 27

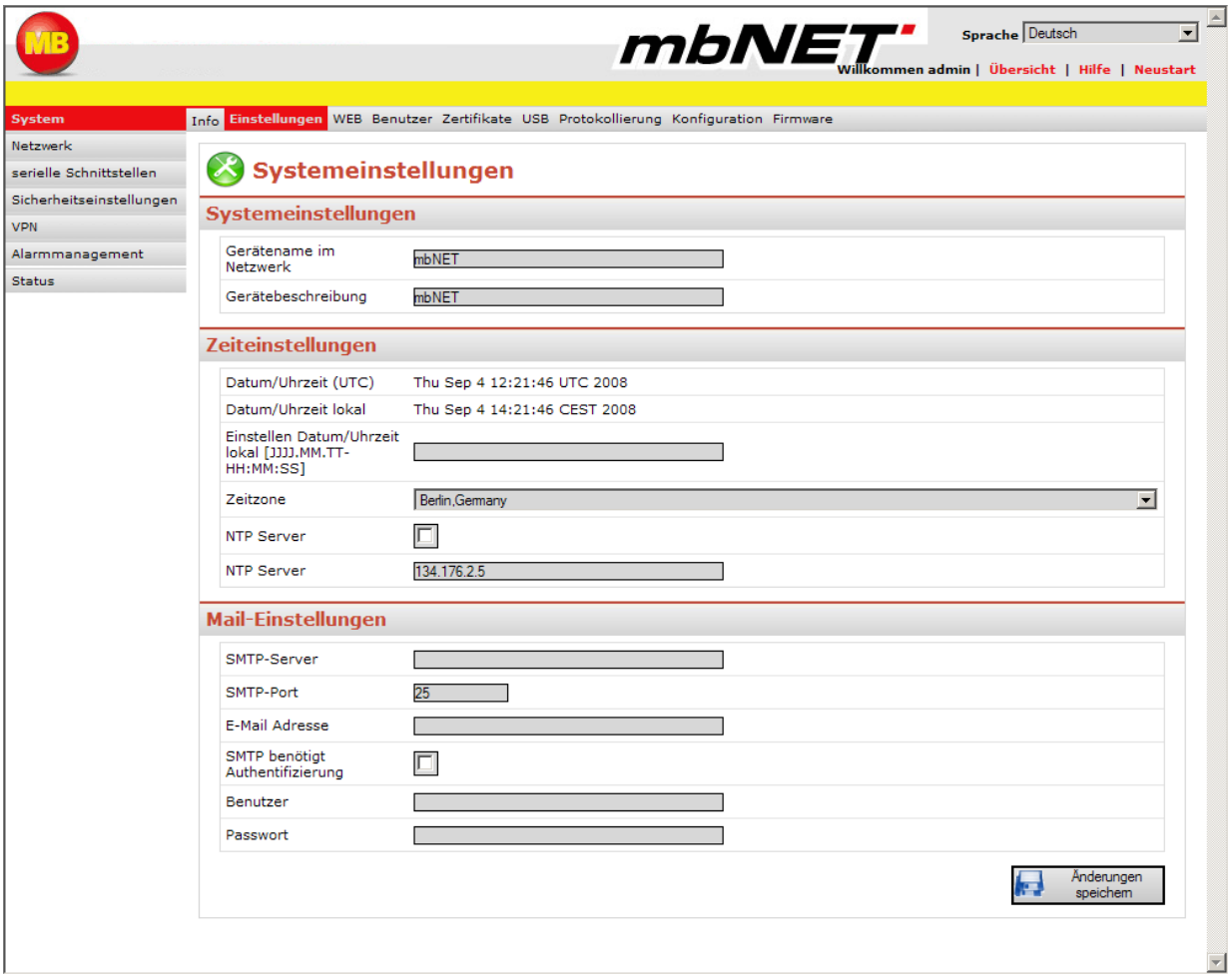


Abbildung 28: Menümaske Systemeinstellungen

Grundkonfiguration des Routers über die Weboberfläche

<table>
<tr><th>Bezeichnung</th><th>Funktion</th></tr>
<tr><td>Gerätename im Netzwerk</td><td>Vergeben Sie einen Namen für den Router.</td></tr>
<tr><td>Gerätebeschreibung</td><td>Um den Router in einem Netzwerk zu identifizieren geben Sie hier eine sinnvolle Beschreibung ein.</td></tr>
<tr><td>Datum / Uhrzeit (UTC)</td><td>Anzeige der aktuellen Systemzeit in Universal Time Coordinates (UTC).</td></tr>
<tr><td>Datum / Uhrzeit lokal</td><td>Anzeige der Uhrzeit anhand der Einstellung der Zeitzone.</td></tr>
<tr><td>Einstellen Datum / Uhrzeit lokal</td><td>Geben Sie hier die Zeit ein, falls kein NTP-Server eingestellt ist bzw. wenn der NTP-Server nicht erreichbar ist. Beispiel: 2007.10.30-13:33:00
<table>
<tr><th>Format</th><th>Bedeutung</th></tr>
<tr><td>JJJJ</td><td>Jahr z.B. 2007</td></tr>
<tr><td>MM</td><td>Monat z.B. 10</td></tr>
<tr><td>TT</td><td>Tag z.B. 30</td></tr>
<tr><td>HH</td><td>Stunde z.B. 13</td></tr>
<tr><td>MM</td><td>Minute z.B. 34</td></tr>
<tr><td>SS</td><td>Sekunde z.B. 48</td></tr>
</table></td></tr>
<tr><td>Zeitzone</td><td>Klicken Sie auf das Auswahlfeld und wählen Sie die Zeitzone aus, in der Sie sich befinden. Eingestellte Zeitzone: Berlin, Germany</td></tr>
<tr><td>NTP-Server</td><td>Wird die Checkbox durch Anklicken mit einem Häkchen versehen, dann bezieht der Router seine Zeit von einem anderen Rechner (falls in nachfolgender Eingabebox eingetragen) und zeigt die aktuelle Systemzeit an.
Die Uhrzeit wird alle zwei Stunden per NTP aktualisiert.
Eingetragener Zeitserver: 134.176.2.5</td></tr>
<tr><td> </td><td>Das mbNET verfügt über eine RTC (gepufferte Uhr). Die eingestellte Uhrzeit wird bis zu 7 Tagen ohne Spannungsversorgung gepuffert</td></tr>
<tr><td>NTP-Server</td><td>Eingabe eines Zeitservers zum Erhalt der aktuellen Systemzeit. Statt des Namens kann auch eine IP-Adresse des Zeitservers eingegeben werden. Bei Eingabe eines Namens muss ein DNS-Server in den Netzwerkeinstellungen eingetragen oder eine Verbindung zum Internet bestehen. Der NTP-Server muss einfach erreichbar sein.</td></tr>
<tr><td>Maileinstellungen</td><td>Wir die Option „automatische Mail-Einstellungen aktivieren“=„Ja“ verwendet, so benutzt der Router feste Vorgaben von MB Connect Line und den Mail-Server von MB Connect Line.</td></tr>
<tr><td>SMTP-Server</td><td>Der SMTP-Server wird benötigt, damit der Router seine Emails versenden kann.</td></tr>
<tr><td>SMTP-Port</td><td>Eingabe des Ports, über den die Emails versendet werden. In der Regel handelt es sich hierbei um den Port 25.</td></tr>
<tr><td>E-Mail Adresse</td><td>Tragen Sie hier die Absenderadresse, als die eigene Emailadresse ein.</td></tr>
<tr><td>SMTP benötigt Authentifizierung</td><td>Abhängig vom Provider ist die Checkbox abzuhaken oder nicht. Erfragen Sie die entsprechende Einstellung bei Ihrem Provider.</td></tr>
<tr><td>Benutzer
Passwort</td><td>Zur Authentifizierung beim SMTP-Server werden Benutzer und Passwort benötigt. D.h. will der Router eine Email an den SMTP loswerden, dann muss er sich gegebenenfalls authentisieren.</td></tr>
</table>

Grundkonfiguration des Routers über die Weboberfläche

8.4 Sicherheitseinstellungen

Um von außen auf die Weboberfläche des Industrierouters zu gelangen ist die eingebaute Firewall des Routers so zu konfigurieren, dass der Port 80 für eingehende Anfragen freigegeben ist.

- ❑ Wechseln Sie hierzu in **Sicherheitseinstellungen** **WAN>LAN**.

- ❑ Klicken Sie auf die Checkbox um diese mit einem Häkchen zu versehen.

Abbildung 29

- ❑ Wählen Sie über das Auswahlfeld die Option **Akzeptieren** aus (Abb. 30).

Abbildung 30

- ❑ Wählen Sie unter **Protokoll** über die Auswahlfläche die Einstellung **tcp** aus.

- ❑ Tragen Sie unter Ziel-Port die Zahl **80** ein.

Abbildung 31

- ❑ Danach speichern Sie Ihre Eingaben mit der Schaltfläche **Änderungen speichern.**

Abbildung 32

- ❑ Zum dauerhaften Abspeichern klicken Sie auf **Änderungen übernehmen.**

Abbildung 33

Grundkonfiguration des Routers über die Weboberfläche

8.4.1 Einstellungen speichern

Wenn Sie die vorher beschriebenen Systemeinstellungen abgeschlossen haben, sichern Sie diese zunächst temporär durch Anklicken der Schaltfläche **Speichern.**

Abbildung 34: Systemeinstellungen temporär speichern

Falls Sie Ihre Eingaben nochmals auf die ursprüngliche Einstellung zurücksetzen wollen, dann betätigen Sie die **Schaltfläche Änderungen löschen.**

Abbildung 35: Systemeinstellungen zurücksetzen

Zur dauerhaften Speicherung der Einstellungen auf dem Industrierouter *mbNET*, klicken Sie jetzt auf die Schaltfläche **Änderungen übernehmen**.

Abbildung 36: Einstellungen auf den Router übertragen

Sollten bestimmte Eingaben fehlen, oder fehlerhaft sein, dann werden die entsprechenden Fehlermeldungen im oberen Bereich der Konfigurationsseite angezeigt. Überprüfen Sie daraufhin nochmals Ihre Einstellungen.

Bitte beachten Sie!
Damit Ihre durchgeführten Einstellungen dauerhaft gespeichert sind und z.B. nach dem Neustart oder Ausschalten des Routers vorhanden sind, müssen Sie grundsätzlich wie oben beschrieben vorgehen. Ansonsten sind Ihre Einstellungen nach dem Ausschalten bzw. nach einem Neustart des Routers verloren.

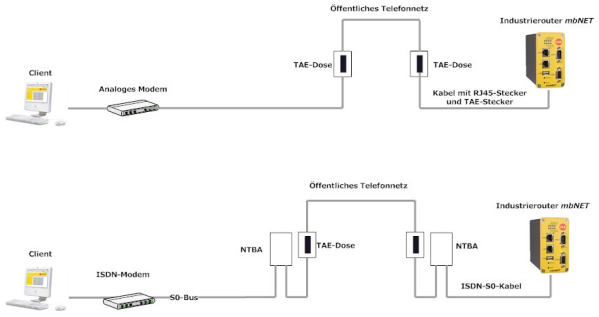
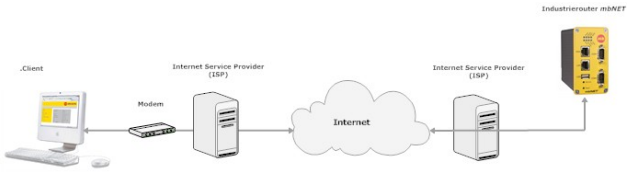
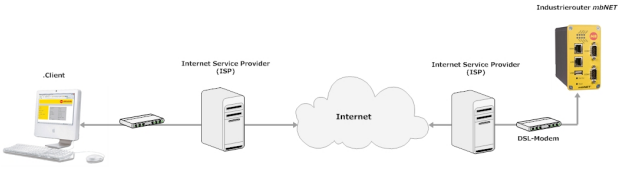
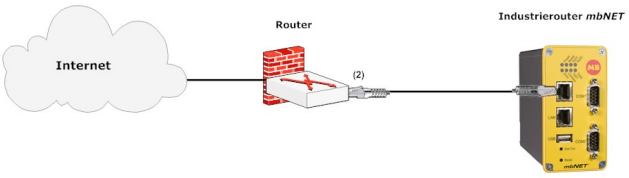
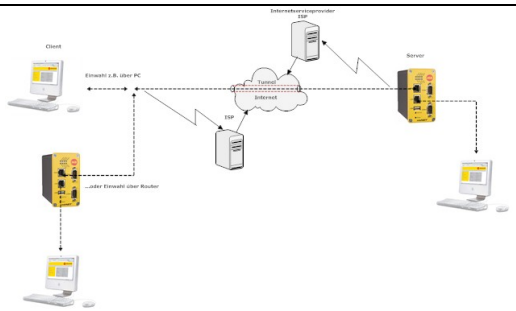
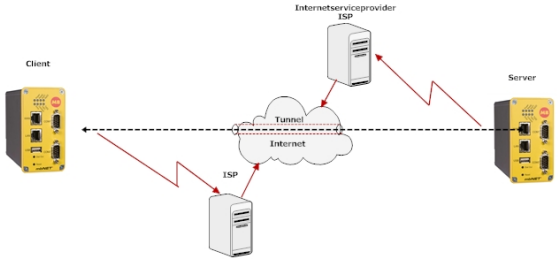
9. Beschreibung verschiedener Verbindungsszenarien

9.1 Allgemeines

Der Router ist nun nach Abschluss der Grundkonfiguration (siehe vorhergehende Seiten) verbindungsabhängig entsprechend anzuschließen und über die Weboberfläche zu konfigurieren.

Nachfolgend die Beschreibung einiger grundlegender Verbindungsszenarien.

Wählen Sie nun unter den nachfolgenden Verbindungsszenarien den für Sie zutreffenden Fall aus und gehen Sie, wie im jeweiligen Kapitel beschrieben, entsprechend vor.

Konfiguration des im Industrierouter mbNET integrierten Modems für eine Verbindung mit einem Client-PC über das öffentliche Telefonnetz (PPP-Einwahl, DFÜ-Netzwerk) **siehe Kapitel 9.2**	
Konfiguration des im Industrierouter mbNET integrierten Modems für eine Verbindung mit einem Client-PC über das Internet **siehe Kapitel 9.3**	
Konfiguration des Industrierouters mbNET für eine Verbindung mit einem Client-PC über einen DSL-Internetzugang unter Verwendung eines DSL-Modems **siehe Kapitel 9.4**	
Konfiguration des Industrierouters mbNET für eine Verbindung ins Internet über einen weiteren Router **siehe Kapitel 9.5**	
Konfiguration des Industrierouters mbNET für eine VPN-Verbindung mit einem Client (Client – Router) **siehe Kapitel 9.6**	
Konfiguration eines Industrierouters mbNET für eine Verbindung zu einem weiteren Industrierouter mbNET per VPN (Router – Router) **siehe Kapitel 9.7**	

9.2 Konfiguration des Industrierouters für eine Verbindung über das Telefonnetz

Die nachfolgende Abbildung zeigt als Beispiel den Anschluss des Industrierouters zum Aufbau einer Verbindung zu einem Client über das **öffentliche Telefonnetz.**
Über diese Art von Verbindung kann über das Telefonnetz auf die seriellen Schnittstellen (siehe Kapitel **Serielle Schnittstellen**) und auf die LAN-Schnittstelle des Industrierouters zugegriffen werden.
Im nachfolgenden Beispiel wird als Client ein PC mit Modemanschluss gewählt.

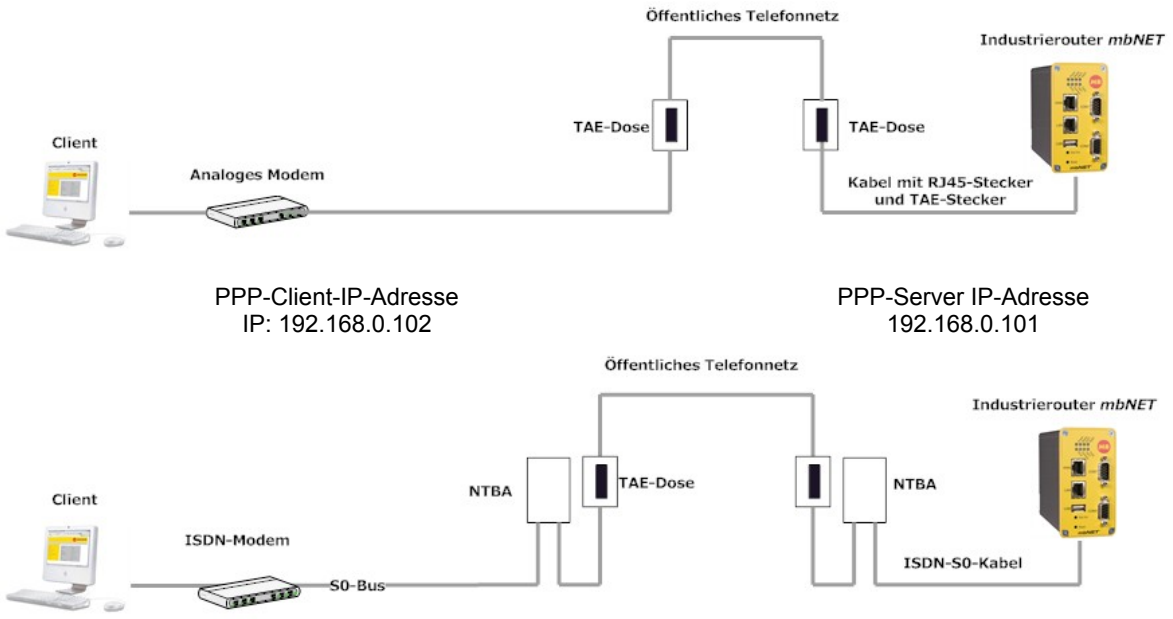


Abbildung 37: Verbindung über das Telefonnetz

Konfiguration der Verbindung über das Telefonnetz (Fortsetzung)

9.2.1 Anschluss und Konfiguration des Routers

Voraussetzung:
Der Router ist bereits an die entsprechende Versorgungsspannung angeschlossen und die beiden grünen LEDs **Power** und **Ready** leuchten konstant.

9.2.1.1 Anschluss des Routers

Bei analogem Anschluss (betrifft die Gerätetypen MDH 600, 610, 620 und MDH 630)

- ❑ Analoges Kabel mit TAE-Adapter verbinden.
- ❑ Stecken Sie das eine Ende des mitgelieferten Kabels in die RJ12-Buchse (**1**) auf der Unterseite des Routers und das andere Ende des Kabels in die TAE-Dose (**2**).

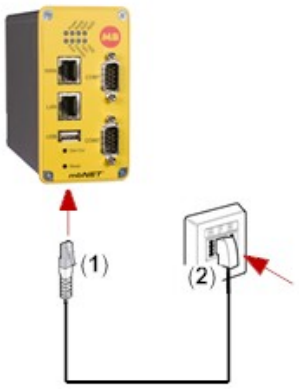


Abbildung 38: Analoger Anschluss

Bei ISDN-Anschluss:
(betrifft die Gerätetypen MDH 602, 612, 622 und MDH 632)

- ❑ Bei vorhandenem **ISDN-Anschluss** stecken Sie das eine Ende des ISDN-Kabels in die Buchse (**1**) auf der Unterseite des Routers und das andere Ende des Kabels in die Buchse (**2**) des **NTBA-Anschlusses.**

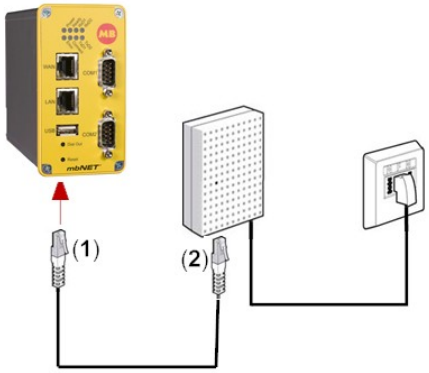


Abbildung 39: ISDN-Anschluss

Bei GSM-Anschluss:
(betrifft die Gerätetypen MDH 603, 613, 623 und MDH 633)

- ❑ Bei vorhandenem **GSM-Anschluss** stecken Sie das eine Ende des GSM-Antennenkabels in die Buchse auf der Unterseite des Routers.

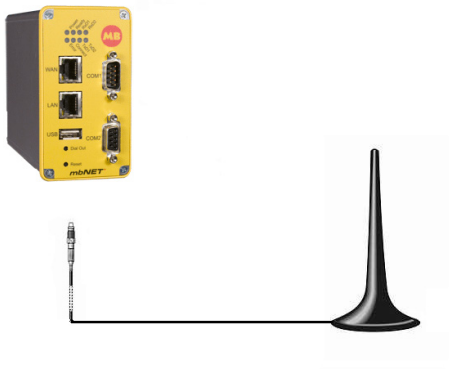


Abbildung 40: GSM-Anschluss

9.2.1.2 Konfiguration des Routers über die Weboberfläche

- ❑ Klicken Sie ausgehend von der Startseite der Weboberfläche auf die Schaltflächen **Netzwerk** – **Modem**.

Abbildung 41

Konfiguration der Verbindung Router – Client über das Telefonnetz

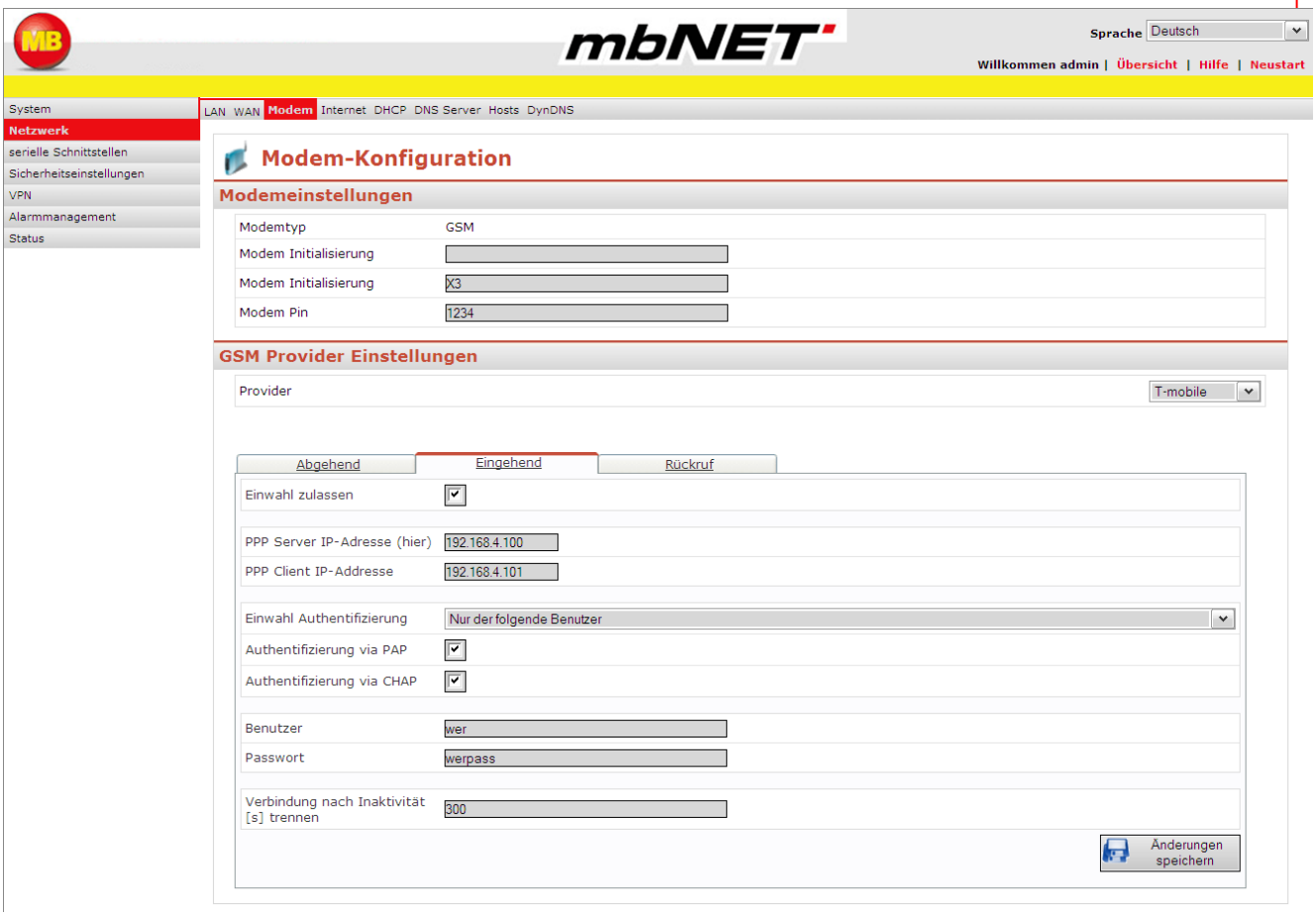


Abbildung 42

Ausführliche und weiterführende Informationen hierzu entnehmen Sie bitte dem Kapitel *Netzwerk - Modem*

Bezeichnung	Beschreibung
Modeminitialisierung	**ANALOG:** Wenn Sie ein analoges Gerät verwenden, dann müssen Sie hier den Befehl **+GCI=Ländercode** (Ländercode siehe Kapitel **Ländercodes für analoge Geräte**) und in die zweite Zeile den Befehl **X3** (nicht auf Freizeichen warten) eingeben. **ISDN:** Wenn Sie ein ISDN-Gerät verwenden, dann müssen Sie mit dem Befehl **AT#Z=n** (n= MSN-Nummer) ihre MSN-Nummer eingeben. Geben Sie für „n“ einen „*“ ein, dann wird jeder Anruf angenommen. **GSM:** Wenn sie ein GSM-Gerät verwenden, dann müssen sie nur den voreingestellten Befehl **X3** beibehalten. Der Befehl **+GCI=Ländercode** darf nicht verwendet werden.
Modem Pin (nur GSM)	Hier können Sie, falls nötig, den PIN für die SIM-Karte eingeben
Provider (nur GSM)	Hier können Sie Ihren Provider auswählen. Für den Fall, dass er nicht vorhanden ist, wählen sie einfach „Other“
Providername (nur GSM)	Falls Ihr Provider nicht in der Auswahl dabei war dann können Sie hier den APN (Access Point Name) auch händisch eingeben. Informationen zum APN erhalten sie von Ihrem Provider.
Eingehend	Klicken Sie auf die Registerkarte **Eingehend.**
Einwahl zulassen	Klicken Sie auf die Checkbox, um diese mit einem Häkchen zu versehen, damit die Einwahl von einem Client möglich ist.
PPP Server IP-Adresse (hier)	Tragen Sie hier die IP-Adresse des Servers in das Eingabefeld ein. Hier: 192.168.0.101
PPP Client IP-Adresse	Tragen Sie die IP-Adresse, die der Client erhalten soll, ein. Hier: 192.168.0.102
Einwahl Authentifizierung	Wählen Sie über das Auswahlfeld **Nur der folgende Benutzer** (hier im Beispiel gewählt) aus.
Authentifizierung via PAP	Übernehmen Sie das standardmäßig eingestellte Authentifizierungsprotokoll. Dies ist z.B. bei der Einrichtung der DFÜ-Verbindung eingerichtet.
Authentifizierung via CHAP	Übernehmen Sie das standardmäßig eingestellte Authentifizierungsprotokoll. Dies ist z.B. bei der Einrichtung der DFÜ-Verbindung eingerichtet.

Fortsetzung Konfiguration der Verbindung Router – Client über das Telefonnetz

Bezeichnung	Beschreibung
Benutzer	Geben Sie den Benutzernamen ein. Hier im Beispiel gewählt: **einwahl**
Passwort	Geben Sie das entsprechende Passwort hierfür ein. Hier im Beispiel gewählt: **einwahl**
Verbindung nach Inaktivität [s] trennen	Tragen Sie hier die Zeit (in Sekunden) ein, nach der die Verbindung abgebaut wird, wenn während dieser Zeit keine Datenübertragung stattfindet. Wenn Sie hier keinen Zahlenwert oder die Zahl „0“ eintragen, dann wird die Verbindung nicht getrennt. Hier im Beispiel gewählt: **300**

- ❑ Speichern Sie jetzt die Änderungen durch Betätigen der Schaltfläche **Änderungen speichern**

- ❑ Klicken Sie nun auf die Schaltflächen **Netzwerk** – **Internet** und führen Sie die nachfolgenden Einstellungen durch.

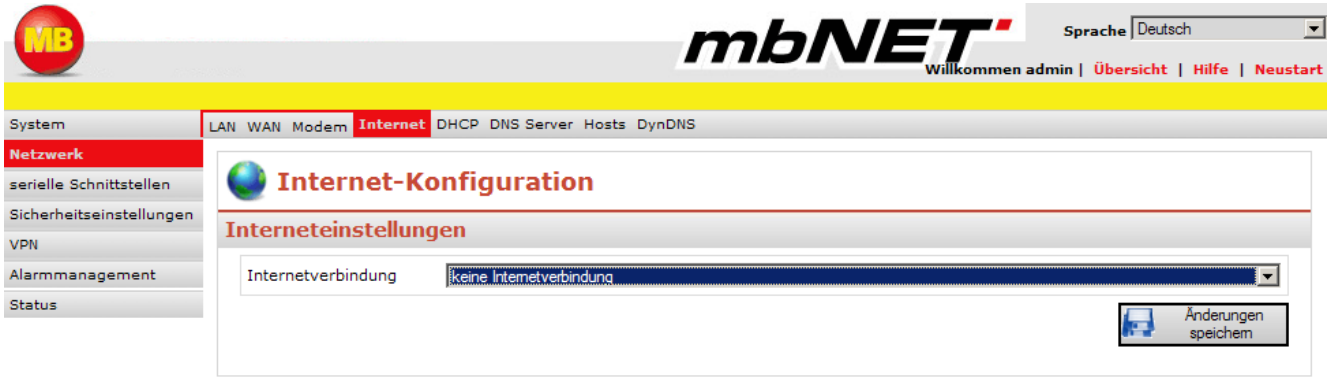


Abbildung 43

Ausführliche Beschreibung der Einstellungen Netzwerk – Internet entnehmen Sie bitte dem Kapitel *Netzwerk - Internet*

Bezeichnung	Beschreibung
Internetverbindung	Wählen Sie über die Auswahlschaltfläche die Option **keine Internetverbindung** oder **Internetverbindung über WAN**.

Fortsetzung Konfiguration der Verbindung Router – Client über das Telefonnetz

- ❑ Speichern Sie die Änderungen durch Anklicken der Schaltfläche **Änderungen speichern.**

Abbildung 44

- ❑ Klicken Sie auf die Schaltflächen **System** - **Benutzer** und legen Sie einen Benutzer mit Einwahlberechtigung an. Weitere Hinweise zum Anlegen eines Benutzers und zur Zuteilung von bestimmten Rechten entnehmen Sie bitte dem ***Kapitel*** ***Benutzer anlegen***

- ❑ Um Ihre Änderungen dauerhaft auf dem Industrierouter zu speichern, klicken Sie zum Schluss auf die Schaltfläche **Änderungen übernehmen.**

Abbildung 45

Hinweis:

- Um Geräte an der LAN-Schnittstelle zu erreichen müssen diese so konfiguriert werden, dass die IP-Adresse der LAN-Schnittstelle des *mbNET*, als Gateway für die Geräte eingetragen wird.
- Der Client darf nicht an einem Netzwerk angeschlossen sein, außer der Adressbereich des Netzwerkes liegt nicht im Bereich der LAN IP-Adresse / WAN IP-Adresse oder der PPP-Verbindung.
- Für die Kommunikation werden nicht die PPP-Adressen verwendet, sondern die LAN IP-Adresse des *mbNET* und die IP-Adressen der daran angeschlossenen Geräte.

Konfiguration der Verbindung Router – Client über das Telefonnetz (Fortsetzung)

9.2.2 Konfiguration eines Clients (PCs) für den Zugriff auf den Router

Sie können sich auf direktem Wege über die Telefonleitung mit dem Router und damit auch mit einem entfernten Netzwerk verbinden. Um auf den Router zuzugreifen muss dieser wie bereits vorher beschrieben entsprechend konfiguriert sein. Danach richten Sie auf dem Rechner eine entsprechende DFÜ-Verbindung gemäß nachfolgender Beschreibung ein.

- ❑ Klicken Sie auf START und dann Systemsteuerung.
- ❑ Klicken Sie auf NETZWERKVERBINDUNGEN und dann auf ASSISTENT FÜR NEUE VERBINDUNGEN. Es startet der Netzwerkverbindungs-Assistent, der alle notwendigen Einstellungen vornimmt.

  Es erscheint der Willkommensbildschirm des Netzwerkverbindungs-Assistenten. Klicken Sie auf **WEITER.**

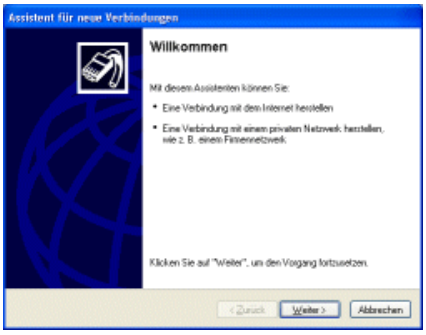

Assistent für neue Verbindungen
Willkommen
Mit diesem Assistenten können Sie:
• Eine Verbindung mit dem Internet herstellen
• Eine Verbindung mit einem privaten Netzwerk herstellen, wie z. B. einem Firmennetzwerk
Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.
< Zurück
Weiter >
Abbrechen

Abbildung 46

- ❑ Im Netzwerkverbindungstyp markieren Sie bitte die zweite Option **Verbindung mit dem Netzwerk am Arbeitsplatz herstellen** und klicken daraufhin auf **WEITER.**

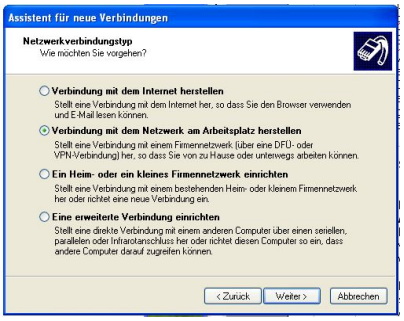

Assistent für neue Verbindungen
Netzwerkverbindungstyp
Wie möchten Sie vorgehen?
Verbindung mit dem Internet herstellen
Stellt eine Verbindung mit dem Internet her, so dass Sie den Browser verwenden und E-Mail lesen können.
Verbindung mit dem Netzwerk am Arbeitsplatz herstellen
Stellt eine Verbindung mit einem Firmennetzwerk (über eine DFÜ- oder VPN-Verbindung) her, so dass Sie von zu Hause oder unterwegs arbeiten können.
Ein Heim- oder ein kleines Firmennetzwerk einrichten
Stellt eine Verbindung mit einem bestehenden Heim- oder kleinem Firmennetzwerk her oder richtet eine neue Verbindung ein.
Eine erweiterte Verbindung einrichten
Stellt eine direkte Verbindung mit einem anderen Computer über einen seriellen, parallelen oder Infrarotanschluss her oder richtet diesen Computer so ein, dass andere Computer darauf zugreifen können.
< Zurück
Weiter >
Abbrechen

Abbildung 47

- ❑ Wählen Sie **DFÜ-Verbindung** und das entsprechende DFÜ-Gerät (Modem) mit dem Sie die Verbindung zum Industrierouter herstellen möchten.

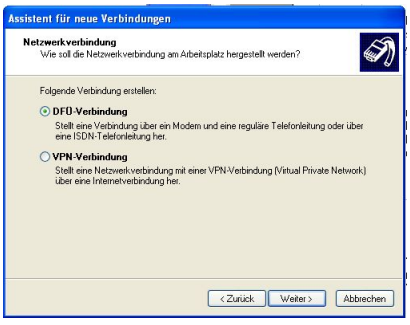

Assistent für neue Verbindungen
Netzwerkverbindung
Wie soll die Netzwerkverbindung am Arbeitsplatz hergestellt werden?
Folgende Verbindung erstellen:
DFÜ-Verbindung
Stellt eine Verbindung über ein Modem und eine reguläre Telefonleitung oder über eine ISDN-Telefonleitung her.
VPN-Verbindung
Stellt eine Netzwerkverbindung mit einer VPN-Verbindung (Virtual Private Network) über eine Internetverbindung her.
< Zurück
Weiter >
Abbrechen

Abbildung 48

Konfiguration der Verbindung Router – Client über das Telefonnetz (Fortsetzung)

- ❑ Jetzt müssen Sie Ihrer Verbindung einen beliebigen Namen geben,
  Danach klicken Sie auf **WEITER.**

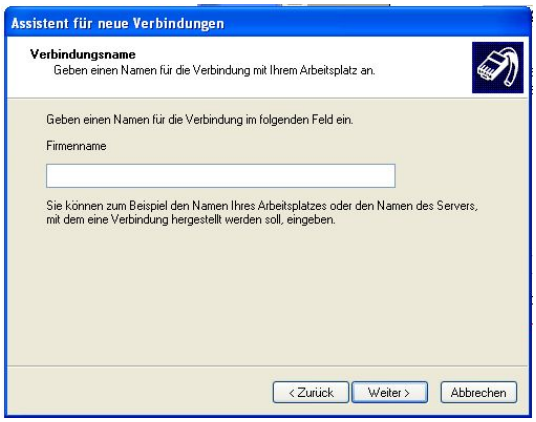

Assistent für neue Verbindungen
Verbindungsname
Geben einen Namen für die Verbindung mit Ihrem Arbeitsplatz an.
Geben einen Namen für die Verbindung im folgenden Feld ein.
Firmenname
Sie können zum Beispiel den Namen Ihres Arbeitsplatzes oder den Namen des Servers, mit dem eine Verbindung hergestellt werden soll, eingeben.
< Zurück
Weiter >
Abbrechen

Abbildung 49

- ❑ Geben Sie die Rufnummer der Gegenstelle ein. (Rufnummer unter der der Industrierouter erreichbar ist)

Assistent für neue Verbindungen
Zu wählende Rufnummer
Welche Rufnummer wird verwendet, um diese Verbindung herzustellen?
Geben Sie die Rufnummer unten ein.
Rufnummer:
Sie müssen eventuell eine "1" bzw. eine Vorwahl oder beides einbeziehen. Wählen Sie die Rufnummer auf Ihrem Telefon, wenn Sie sich nicht sicher sind, ob diese zusätzlichen Nummern erforderlich sind. Die gewählte Nummer ist korrekt, wenn Sie bei dem Telefonanruf einen Modemton hören.
< Zurück
Weiter >
Abbrechen

Abbildung 50

- ❑ Klicken Sie auf **Fertig stellen**.

Assistent für neue Verbindungen
Fertigstellen des Assistenten
Die erforderliche Schritte zum Erstellen der folgenden Verbindung wurden ordnungsgemäß durchgeführt:
DFÜ-Verbindung
• Für alle Benutzer dieses Computers freigeben
Die Verbindung wird im Ordner "Netzwerkverbindungen" gespeichert.
Verknüpfung auf dem Desktop hinzufügen
Klicken Sie auf "Fertig stellen", um diese Verbindung zu erstellen und den Vorgang abzuschließen.
< Zurück
Fertig stellen
Abbrechen

Abbildung 51

Konfiguration der Verbindung Router – Client über das Telefonnetz (Fortsetzung)

9.2.3 Verbindung vom Client-PC zum Industrierouter aufbauen

- ❑ Doppelklicken Sie auf die Verbindung die Sie auf den vorhergehenden Seiten erstellt haben.
- ❑ Geben Sie in diesem Fenster jetzt den **Benutzernamen** und das **Kennwort** ein, welche Sie bei der Konfiguration des Modems bereits vorher festgelegt haben.

Die standardmäßigen Einstellungen **Authentifizierung via CHAP** und **Authentifizierung via PAP** müssen mit den Einstellungen am Industrierouter übereinstimmen, da sonst keine Verbindung hergestellt werden kann.

- ❑ Betätigen Sie die Schaltfläche **Wählen.**

✓ **Die Verbindung wird zum Industrierouter aufgebaut**

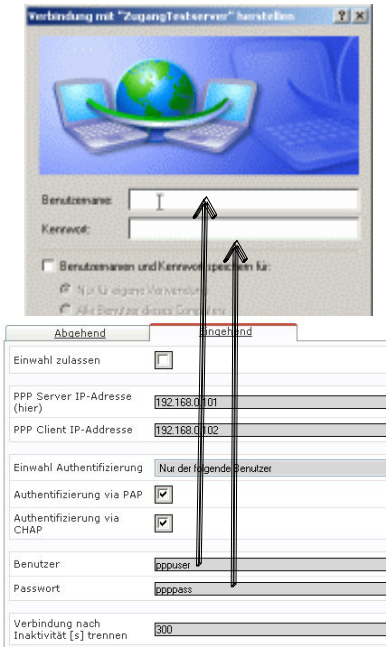


Abbildung 52

9.2.4 Anzeigen und Überprüfen des Verbindungsstatus

Über einen an der LAN-Schnittstelle des Routers angeschlossenen PC können Sie sich nach Betätigen der Schaltflächen **Status** – **Modem** anzeigen lassen, ob sich ein Benutzer eingewählt hat und bei hergestellter Verbindung, wer sich auf den Router eingewählt hat.

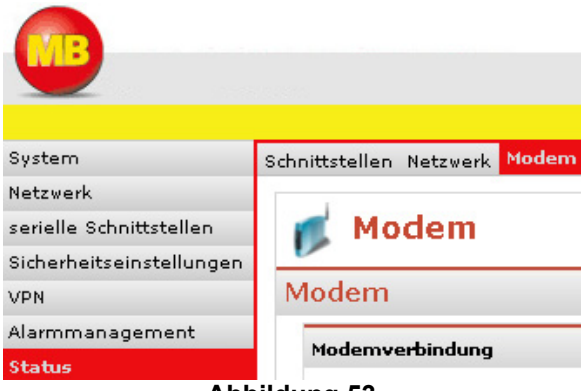


Abbildung 53

9.3 Konfiguration des Industrierouters für eine Verbindung mit dem Internet

Die nachfolgende Abbildung zeigt die Verbindung des Industrierouters über das Internet zu einem Client. Als Client dient ein PC mit Modemanschluss.

Bei dieser Verbindung kann nur auf die seriellen Schnittstellen zugegriffen werden (Schnittstellenbeschreibung siehe Kapitel Serielle Schnittstellen). Der Zugriff auf die LAN-Schnittstelle des Industrierouters ist nur durch Port-Forwarding möglich.

Der Zugriff auf eine LAN-Schnittstelle über eine Internetverbindung ist nur über eine VPN-Verbindung (Beschreibung VPN-Verbindung siehe Kapitel **Konfiguration des Industrierouters für eine VPN-Verbindung mit einem Client**) möglich.

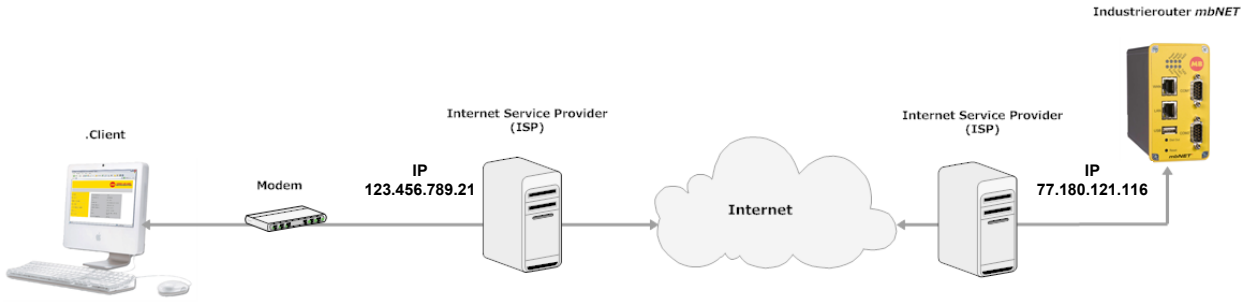


Abbildung 54

Konfiguration einer Verbindung mit dem Internet (Fortsetzung)

9.3.1 Anschluss und Konfiguration des Routers

Voraussetzung:
Der Router ist bereits an die entsprechende Versorgungsspannung angeschlossen und die grünen Leuchtdioden **Power** und **Ready** leuchten konstant.

9.3.1.1 Anschluss des Routers

Nur bei analogem Anschluss (betrifft die Gerätetypen MDH 6x0)

- ❑ Analoges Kabel mit dem TAE-Adapter verbinden.
- ❑ Stecken Sie das mitgelieferte Kabel auf der einen Seite in die RJ12-Buchse (**1**) des Routers und das andere Ende des Kabels in den TAE-Dose (**2**).

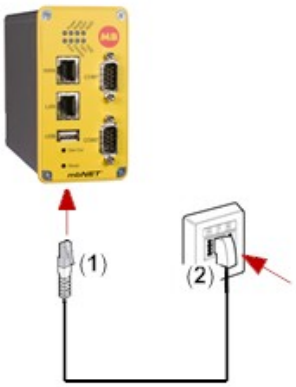


Abbildung 55: Analoger Anschluss

Nur bei ISDN-Anschluss (betrifft die Gerätetypen MDH6x2)

- ❑ Stecken Sie das eine Ende des mitgelieferten Kabels in die Buchse (**1**) und das andere Ende des Kabels in die Buchse (**2**) des **NTBA-Anschlusses.**

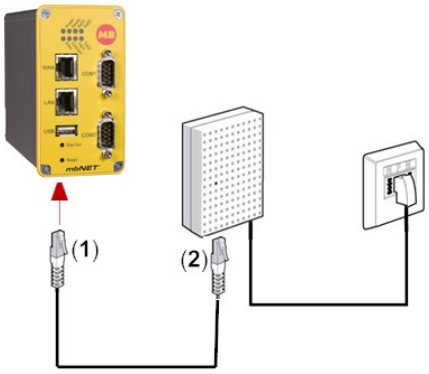


Abbildung 56: ISDN-Anschluss

Nur bei GSM-Anschluss (betrifft die Gerätetypen MDH6x3 und 6x4)

- ❑ Stecken Sie das eine Ende des mitgelieferten Antennenkabels in die Buchse.

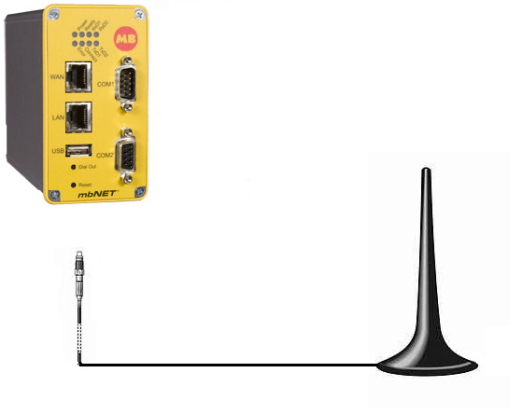


Abbildung 57: GSM-Anschluss

9.3.1.2 Konfiguration des Routers über die Weboberfläche

- Mit dem Verbindungsassistent können Sie ihre Verbindungen schnell und einfach konfigurieren. Klicken Sie dazu auf der Weboberfläche rechts oben auf den Link Assistenten. Wenn Sie die Funktion des automatischen Öffnens des Assistenten deaktiviert haben, dann klicken Sie auf den Start-Knopf des Assistenten für Internetverbindungen.

Abbildung 58:

- ❑ Wählen Sie hier die Option Modem aus und klicken auf „Weiter“
- ❑ Es ist schon ein Internetanbieter im mbNET hinterlegt, klicken Sie hierzu auf „Voreingestellter Anbieter“ Jedoch können Sie auch einen eigenen auswählen, dazu müssen Sie „Anbieter manuell auswählen“ und eigene Daten ihres Anbieters eintragen.
- ❑ Sollte das mbNET hinter einer Telefonanlage betrieben werden, so aktivieren Sie die Box neben „Folgende Amtsholung verwenden“ und danach auf „Weiter“
- ❑ Im Anschluss können Sie noch wählen, ob Ihnen das mbNET eine Email mit der aktuellen, öffentliche Adresse schicken, ein dynamischen DNS-Dienst verwendet oder über den DynDNS von MB Connect Line im Internet erreichbar sein soll.

Für eine manuelle Konfiguration gehen Sie wie folgt vor:

Ausgehend von der Startseite klicken Sie auf die Schaltflächen **Netzwerk** und **Modem** und dann auf die Registerkarte Abgehend.

- ❑ Es wird die nachfolgende Bildschirmmaske (siehe nachfolgende Seite) angezeigt.
  Gehen Sie entsprechend den Beschreibungen auf den nachfolgenden Seiten vor.

Abbildung 59

Konfiguration einer Verbindung mit dem Internet (Fortsetzung)

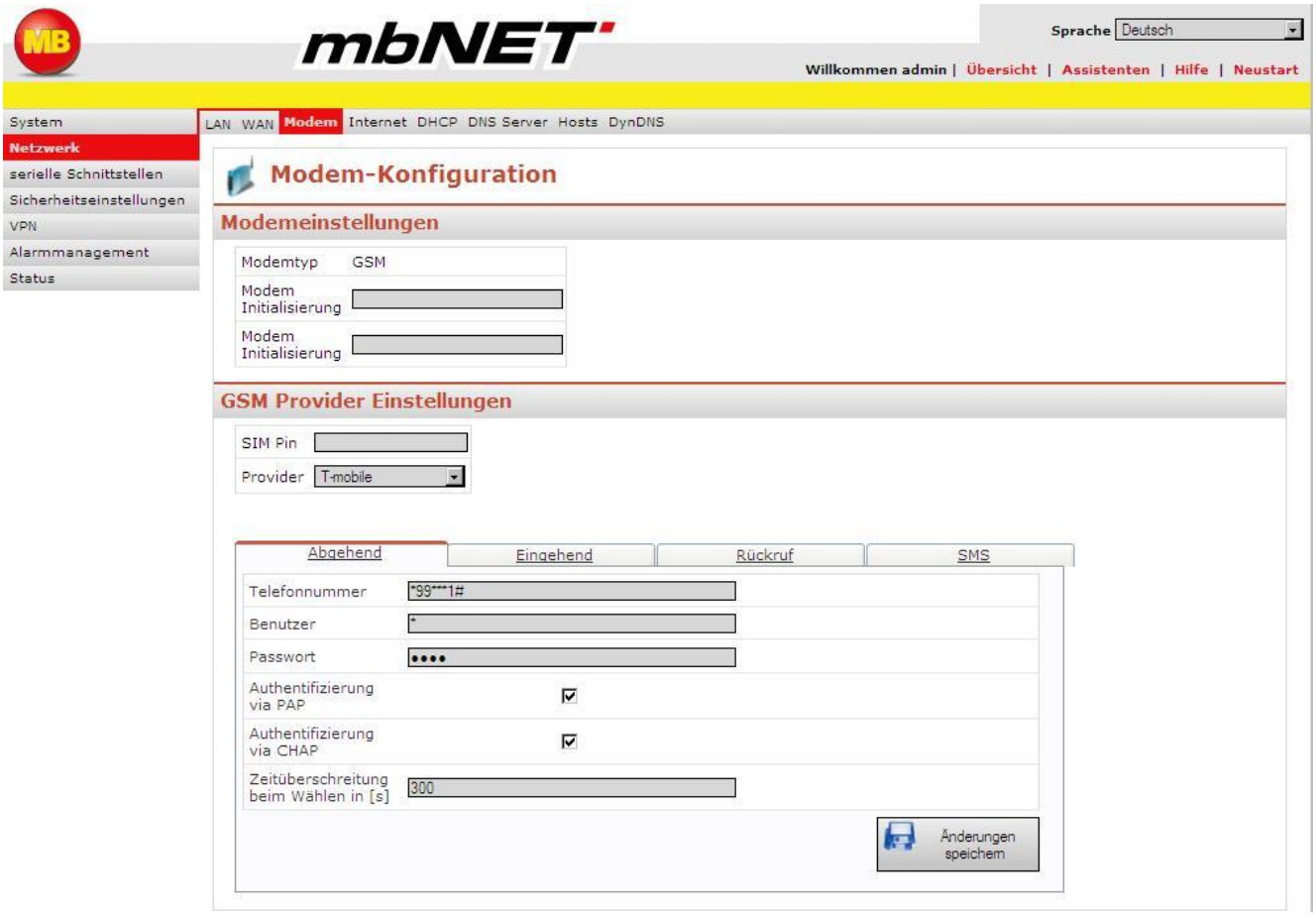


Abbildung 60

Ausführliche Beschreibung der Einstellungen Netzwerk – Modem entnehmen Sie bitte dem Kapitel *Netzwerk - Modem*

Bezeichnung	Beschreibung
Modeminitialisierung	**ANALOG:** Wenn Sie ein analoges Gerät verwenden, dann müssen Sie hier den Befehl **+GCI=Ländercode** (Ländercode siehe Kapitel **Ländercodes für analoge Geräte**) und in die zweite Zeile den Befehl **X3** (nicht auf Freizeichen warten) eintragen. **ISDN:** Wenn Sie ein ISDN-Gerät verwenden, dann müssen Sie mit dem Befehl **AT#Z=n** (n= MSN-Nummer) ihre MSN-Nummer eingeben. Geben Sie für „n“ einen „*“ ein, dann wird jeder Anruf angenommen. **GSM:** Wenn Sie ein GSM-Gerät verwenden, dann müssen Sie nur den voreingestellten Befehl X3 beibehalten. Der Befehl **+GCI=Ländercode** darf nicht verwendet werden.
Modem PIN (nur GSM)	Hier können Sie, falls nötig, den PIN der SIM-Karte eintragen.

Provider (nur GSM)	Hier können Sie Ihren Provider auswählen. Ist er nicht vorhanden, so können Sie den APN (Access Point Name) auch selbst eintragen. Informationen zum APN finden Sie auf unserer Internetseite () oder bei ihrem Mobilfunkanbieter.
Providername	Falls sie unter Provider keinen passenden Eintrag finden, dann können Sie hier Ihren APN händisch eintragen. Fragen Sie Ihren Anbieter wie der APN-Eintrag aussehen muss oder suchen Sie danach im Internet.
Telefonnummer	Geben Sie hier die Rufnummer des entsprechenden Providers ein. Zum Beispiel die Einwahlnummer von Iby-Call: 019193384 **Beachten Sie dabei den Vermerk unten!** Bei **GSM**-Modems lautet die Einwahlnummer immer ***99#**
Benutzer	Eingabe des Benutzernamens (den Providerdaten entnehmen). Hier im Beispiel gewählt: smart86 Bei GSM-Modems finden sie z.B. unter http://www.teltarif.de/i/gprs-config.html die nötigen Informationen (meist ist der Benutzername beliebig).
Passwort	Eingabe des Passwortes (den Providerdaten entnehmen). Hier im Beispiel gewählt: beliebig Bei GSM-Modems finden sie z.B. unter http://www.teltarif.de/i/gprs-config.html die nötigen Informationen (meist ist das Passwort beliebig).
Authentifizierung via PAP	Übernehmen Sie das standardmäßig eingestellte Authentifizierungsprotokoll. Dies ist standardmäßig bei der Einrichtung einer DFÜ-Verbindung eingerichtet.
Authentifizierung via CHAP	Übernehmen Sie das standardmäßig eingestellte Authentifizierungsprotokoll. Dies ist z.B. bei der Einrichtung der DFÜ-Verbindung eingerichtet.
Zeitüberschreitung beim Wählen in [s]	Geben Sie eine Zeit von 300 (=5 Minuten hier im Beispiel gewählt) ein, nach der der Wählvorgang abgebrochen wird.

- ❑ Speichern Sie die Änderungen durch Anklicken der Schaltfläche **Änderungen speichern.**

Abbildung 61

Bitte beachten Sie folgenden Vermerk:

Die Internet-by-call Anbieter wechseln des Öfteren ihre Tarife. MB Connectline kann für eventuelle Preisänderungen nicht verantwortlich gemacht werden.

Konfiguration einer Verbindung mit dem Internet (Fortsetzung)

- ❑ Ausgehend von der Startseite der Weboberfläche, klicken Sie auf die Schaltflächen **Netzwerk** und **Internet**

  Es wird die nachfolgende Bildschirmmaske angezeigt.
  Gehen Sie entsprechend der folgenden Beschreibung vor.

Abbildung 62

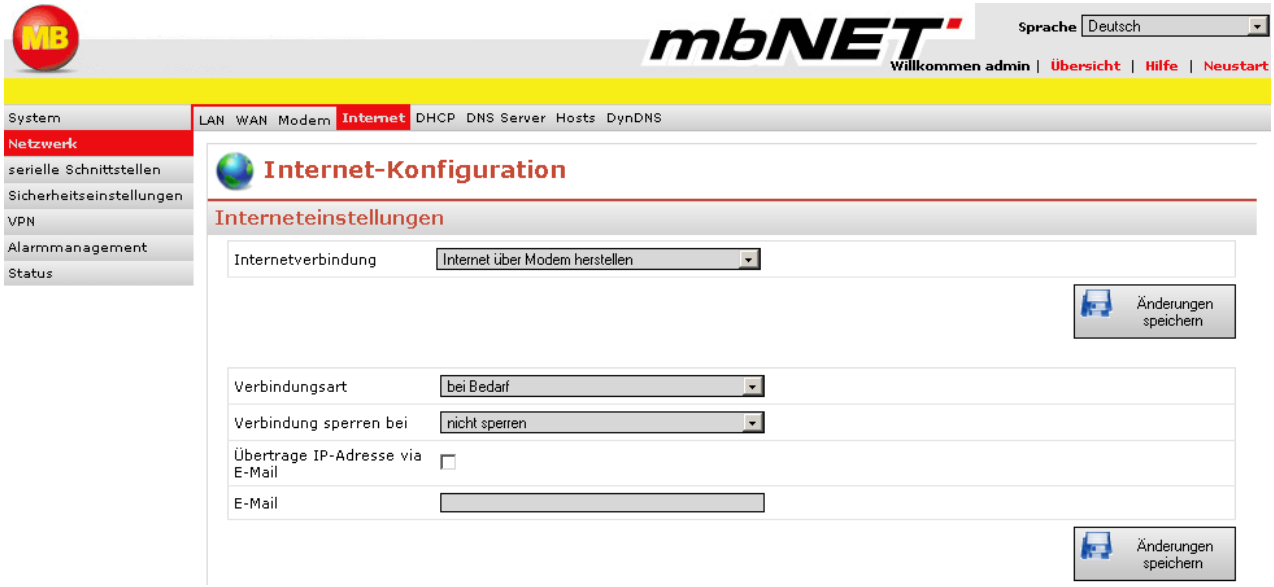


Abbildung 63

Ausführliche Beschreibung der Einstellungen im Kapitel Netzwerk - Internet

Pos.	Bezeichnung	Beschreibung
1	**Internetverbindung**	Wählen Sie über das Auswahlfeld die Einstellung. **Internet über Modem herstellen**
2	**Verbindungsart**	Wählen Sie **Verbindung immer aufrechterhalten**
3	**Verbindung sperren bei**	Über das Auswahlfeld können Sie entscheiden, ob die Verbindung ins Internet durch Aufschalten eines Signals (zwischen 10 und 30V intern generiert) an einem der Eingänge getrennt werden soll.
4	**Übertrage IP-Adresse via E-Mail**	Aktivieren Sie diese Einstellung. Wählen Sie aus, ob die IP-Adresse an die nachfolgend aufgeführte Emailadresse gesendet werden soll.
5	**E-Mail**	Tragen Sie hier die Emailadresse ein, an die die IP-Adresse gesendet werden soll.

- ❑ Speichern Sie die Änderungen durch Anklicken der Schaltfläche **Änderungen speichern.**
- ❑ Um Ihre Änderungen dauerhaft auf dem Industrierouter zu speichern, klicken Sie zum Schluss auf die Schaltfläche **Änderungen übernehmen.**

Abbildung 64

Konfiguration einer Verbindung mit dem Internet (Fortsetzung)

9.3.2 Einwahl Router ins Internet

Der Router ist in der vorherigen Bildschirmmaske so konfiguriert, dass er eine Verbindung ins Internet aufbaut, sobald er neu gestartet wird.

Weitere Möglichkeiten der Einwahl ins Internet entnehmen Sie bitte dem Kapitel **Netzwerk - Internet**

Abbildung 65

- **IP-Adresse übermitteln**
  Für den Zugriff des Clients auf den Router muss die IP-Adresse unter der der Router erreichbar ist, bekannt sein**.** Gemäß vorheriger Konfiguration wird die IP-Adresse an die eingegebene Emailadresse versendet. Sie können somit auf den Router über die IP-Adresse zugreifen.

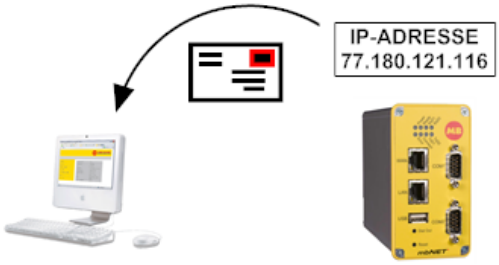


Abbildung 66

Da sich die IP-Adresse des Routers bei jeder Einwahl ins Internet ändert, bietet sich als Alternative an, den **DynDNS-Dienst** unserer Firma iin Anspruch zu nehmen. Informationen zur Einrichtung und Nutzung des DynDNS-Dienstes von MB Connect Line entnehmen Sie bitte dem **Kapitel** ***Netzwerk - DynDNS***

9.3.3 Anzeigen der Internetverbindung

Zugriff auf den Router vorausgesetzt kann man sich durch Betätigen der Schaltflächen **Status** – **Internet** über den Internetstatus informieren.

Abbildung 67

Informationen zu den Statusmeldungen entnehmen Sie bitte dem Kapitel ***Statusmeldungen***

9.4 Konfiguration des Industrierouters unter Einsatz eines DSL-Modem für eine Verbindung mit dem Internet

Die nachfolgende Abbildung zeigt das Anschlussprinzip des Industrierouters *mbNET* zum Aufbau einer Verbindung mit einem Client per DSL-Modem über das Internet.
Vom Client aus ist eine bestehende Verbindung ins Internet zu verwenden, bzw. eine Verbindung ins Internet einzurichten.

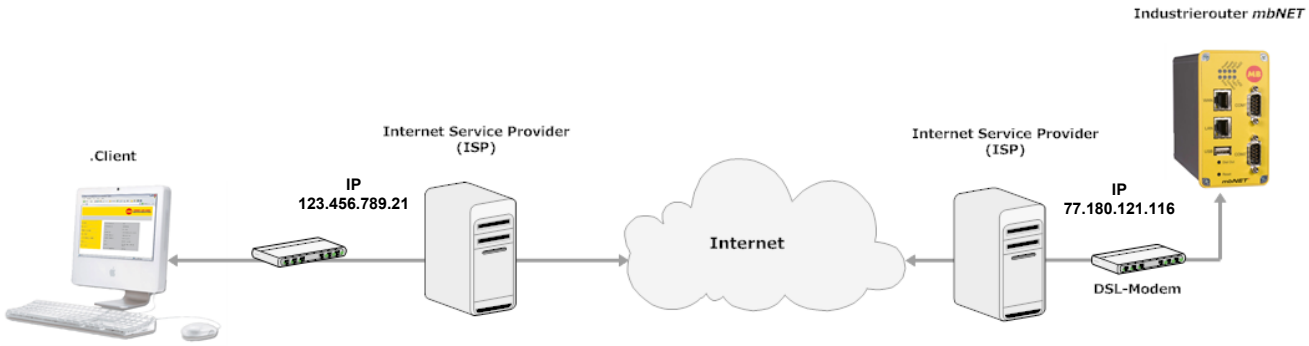


Abbildung 68

Konfiguration einer Verbindung mit dem Internet (Fortsetzung)

9.4.1 Anschluss und Konfiguration des Routers

Voraussetzung:
Der Router ist bereits an die entsprechende Versorgungsspannung angeschlossen und die grünen Leuchtdioden **Power** und **Ready** leuchten konstant.

9.4.1.1 Anschluss des Routers

- ❑ Schließen Sie den Router wie in der Abbildung rechts dargestellt an das DSL-Modem an.
- ❑ Stecken Sie hierzu das eine Ende des Netzwerkkabels (Belegung 1zu1) in die Buchse LAN (1) des DSL-Modems und das andere Ende (2) in die Buchse WAN des Routers.

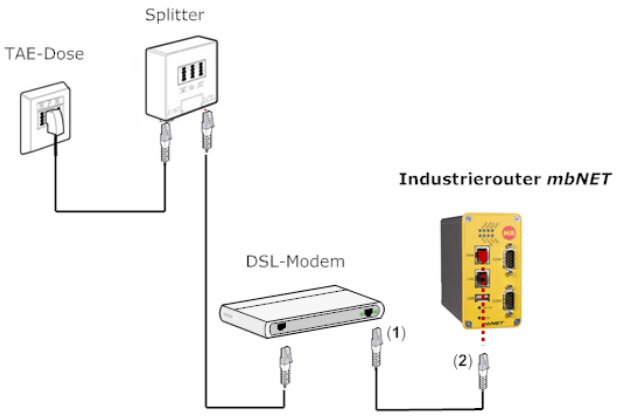


Abbildung 69: Anschluss des Routers

9.4.1.2 Konfiguration des Routers über die Weboberfläche

- ❑ **Mit dem Verbindungs-assistent** können Sie ihre Verbindungen schnell und einfach konfigurieren. Klicken Sie dazu rechts oben auf den Link Assistenten. Wenn Sie die Funktion des automatischen Öffnens des Assistenten deaktiviert haben, dann klicken Sie auf den Start-Knopf des Assistenten für Internetverbindungen.

- ❑ Wählen Sie nun die Option externes DSL-Modem aus.

- ❑ Geben Sie danach ihre Internetzugangsdaten ein. Diese erhalten Sie von ihrem Internet-Dienstanbieter

- ❑ Im Anschluss können Sie noch wählen, ob Ihnen das mbNET eine Email schicken, über dynamischen DNS-Dienst verwendet oder über den DynDNS von MB Connect Line im Internet erreichbar sein soll

- ❑ Bestätigen Sie ihre Eingaben zum Abschluss um diese zu speichern. Schließlich muss das mbNET neu gestartet werden, damit die Einstellungen komplett übernommen werden

- ❑ Betätigen Sie ausgehend von der Startseite der Konfigurationsoberfläche die Schaltflächen **Netzwerk** – **WAN** und dann auf die Registerkarte Schnittstelle. Es wird die nachfolgende Abbildung dargestellt. Gehen Sie laut nachfolgender Beschreibung weiter vor.

Abbildung 70

Konfiguration einer Verbindung mit dem Internet (Fortsetzung)

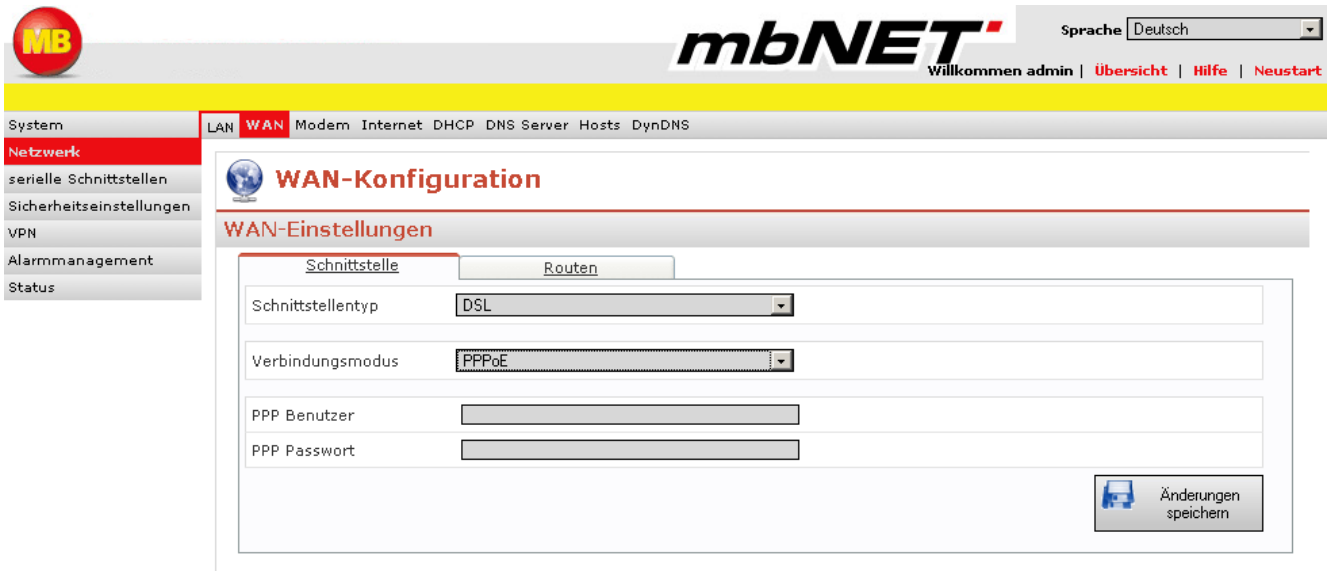


Abbildung 71

Ausführliche Beschreibung der Einstellungen Netzwerk – WAN entnehmen Sie bitte dem Kapitel *Netzwerk - WAN*

Bezeichnung	Beschreibung
Schnittstellentyp	Wählen Sie hier die Option **DSL** aus.
Verbindungsmodus	Wenn sie sich in Deutschland befinden, wählen Sie **PPPoE** (meist verwendetes Protokoll in Deutschland). Das PPTP-Protokoll wird meist in Österreich verwendet.
PPP Benutzer	Geben Sie hier Ihren Benutzernamen für den Internetzugang ein. Entnehmen Sie den Benutzernamen den Zugangsdaten Ihres Internet-Service-Providers.
PPP Passwort	Geben Sie hier Ihr Passwort für ihren Internetzugang ein. Entnehmen Sie das Passwort den Zugangsdaten Ihres Providers.

- ❑ Speichern Sie die Änderungen durch Anklicken der Schaltfläche **Änderungen speichern.**

Abbildung 72

Konfiguration einer Verbindung mit dem Internet (Fortsetzung)

- ❑ Ausgehend von der Startseite der Weboberfläche klicken Sie auf die Schaltflächen **Netzwerk** - **Internet.**

- ❑ Es wird die nachfolgende Bildschirmmaske angezeigt.
  Gehen Sie folgendermaßen vor:

Abbildung 73

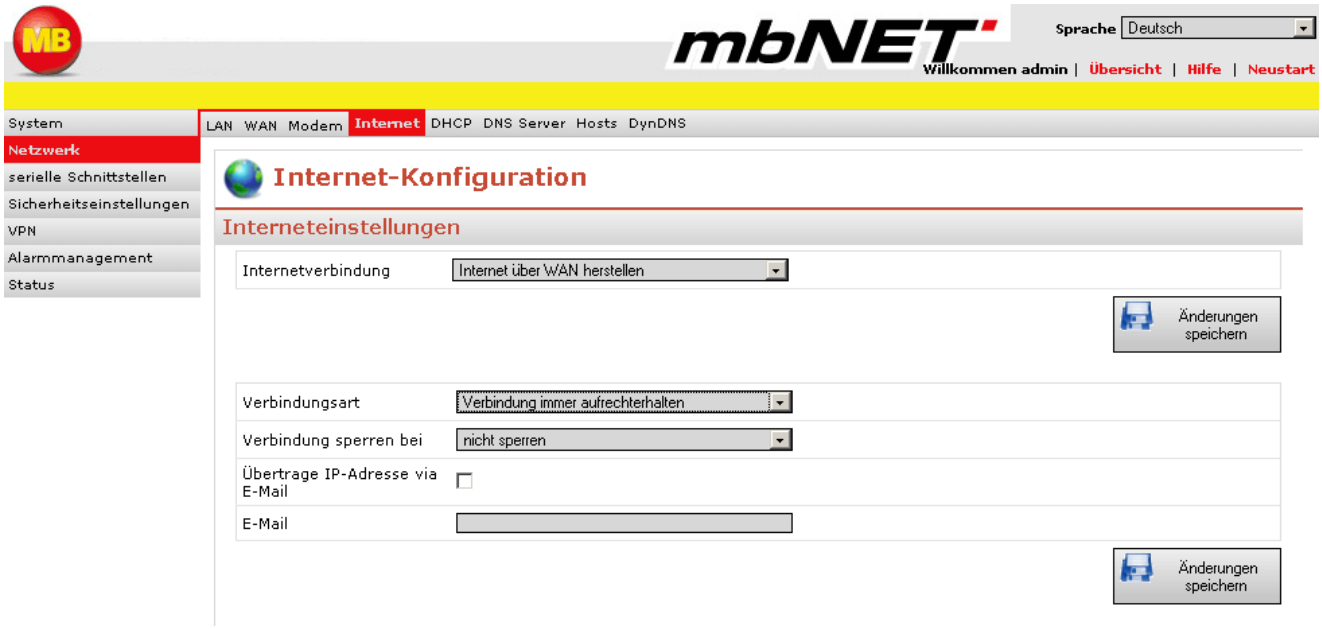


Abbildung 74

Ausführliche Beschreibung der Einstellungen Netzwerk – Internet entnehmen Sie bitte dem Kapitel *Netzwerk - Internet*

Bezeichnung	Beschreibung
Internetverbindung	Wählen Sie hier die Einstellung **Internet über WAN herstellen** aus.
Verbindungsart	Wählen Sie **Verbindung aufrechterhalten.** Die Verbindung wird durch Neustart hergestellt.
Verbindung sperren bei	Sie können die Verbindung zum Internet mittels eines Signals an einem der digitalen Eingänge unterbrechen
Übertrage IP-Adresse via E-Mail	Checkbox durch Anklicken mit Häkchen versehen, um die IP-Adresse unter der der Router erreichbar ist, an die nachfolgend einzutragende Email zu senden.
E-Mail	An die hier angegebene Adresse wird eine Nachricht versendet, wenn eine Internetverbindung aufgebaut wurde.

Konfiguration einer Verbindung mit dem Internet (Fortsetzung)

- ❑ Speichern Sie die Änderungen durch Anklicken der Schaltfläche **Änderungen speichern.**

- ❑ Um Ihre Änderungen dauerhaft auf dem Industrierouter zu speichern, klicken Sie zum Schluss auf die Schaltfläche **Änderungen übernehmen.**

- ❑ Anschließend müssen Sie den ***Router Neustarten***.

Abbildung 75

9.4.2 Verbindung zwischen Client-PC und Router herstellen

- ❑ Einwahl Router ins Internet. Abhängig von den Einstellungen im Router (siehe Internet-Konfiguration) stellen Sie eine Internetverbindung des Routers durch Neustart bzw. Betätigen der Taste Reset her.

Abbildung 76

Weitere Einstellungen bezüglich Interneteinwahl entnehmen Sie bitte dem Kapitel Netzwerk - Internet

- ❑ Einwahl Client-PC ins Internet. Einwahl des Client-PCs ins Internet durchführen.

Abbildung 77

- ❑ IP-Adresse übermitteln
  Für den Zugriff des Client-PCs auf den Router muss die IP-Adresse unter der der Router erreichbar ist, bekannt sein. Bei der Routerkonfiguration ist die Übertragung der IP-Adresse ausgewählt. Die IP-Adresse wird an die in der Routerkonfiguration eingestellte Emailadresse versendet und ist damit bekannt.

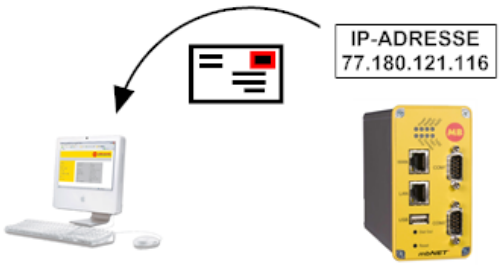


Abbildung 78

Da sich die IP-Adresse des Routers bei jeder Einwahl ins Internet ändert, bietet es sich an, als Alternative den **DynDNS-Dienst** unserer Firma in Anspruch zu nehmen.
Informationen zur Einrichtung und Nutzung des DynDNS-Dienstes von MB Connect Line entnehmen Sie bitte dem Kapitel Netzwerk - DynDNS

9.4.3 Anzeigen des Verbindungsstatus

- ❑ Über die Schaltflächen **Status** – **Internet** können Sie bei einem am LAN-Anschluss angeschlossen PC kontrollieren, ob eine Verbindung ins Internet aktiv ist.

Abbildung 79

Weitere Informationen zu den Statusmeldungen entnehmen Sie bitte dem Kapitel Statusmeldungen

9.5 Konfiguration des Industrierouters bei bereits bestehendem Router für eine Verbindung ins Internet

Die nachfolgende Abbildung zeigt den Anschluss des Industrierouters in einem Netzwerk an einem bereits vorhandenen Router, der bereits für die Verbindung ins Internet zuständig ist. Hierzu muss der bereits vorhandene Router entsprechend eingestellt sein. Diese Betriebsart ist hauptsächlich sinnvoll, wenn man vom Industrierouter *mbNET* zu einem VPN-Gateway eine Verbindung aufbauen möchte.

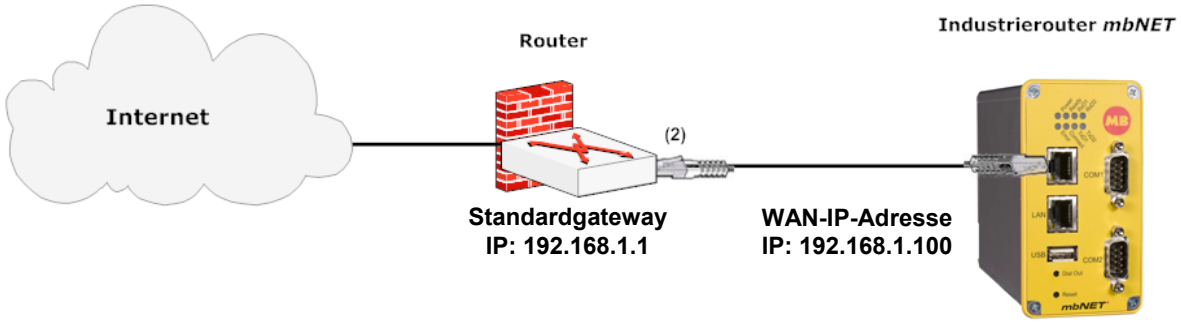


Abbildung 80

Konfiguration des Routers bei bestehendem Router für eine Verbindung ins Internet

9.5.1 Anschluss und Konfiguration des Routers

9.5.1.1 Anschluss des Routers

- ❑ Verbinden Sie den Router wie in der Abbildung rechts dargestellt mit dem bereits vorhandenen Router.
  - ❑ Stecken Sie hierzu das eine Ende des Netzwerkkabels (**1**) (gekreuztes Netzwerkkabel) in die Buchse (**1**) **WAN** des Routers *mbNET* und das andere Ende in die **LAN**-Buchse (**2**) des bereits im Netzwerk vorhandenen Routers.

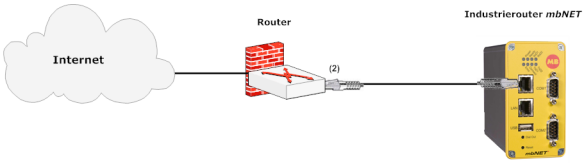


Abbildung 81

9.5.1.2 Konfiguration des Routers über die Weboberfläche

- **Mit dem Verbindungs-assistent** können Sie ihre Verbindungen schnell und einfach konfigurieren. Klicken Sie dazu rechts oben auf den Link Assistenten. Wenn Sie die Funktion des automatischen Öffnens des Assistenten deaktiviert haben, dann klicken Sie auf den Start-Knopf des Assistenten für Internetverbindungen.

- Wählen Sie nun die Option „externer Router (Firewall)“ aus

- Danach haben Sie die Wahl zwischen automatischer Erkennung und manueller Eingabe ihrer Netz-/ und Schnittstellendaten.

- Lesen Sie sich die Informationen durch und nach einem weiteren Klick auf „Weiter“ können Sie den Assistenten mit „Fertigstellen“ beenden. Schließlich ist ein Neustart erforderlich

- Betätigen Sie ausgehend von der Startseite der Konfigurationsoberfläche die Schaltflächen **Netzwerk** - **WAN** – **Schnittstelle**. Es wird die nachfolgende Abbildung dargestellt.

Abbildung 82

Konfiguration des Routers bei bestehendem Router für eine Verbindung ins Internet

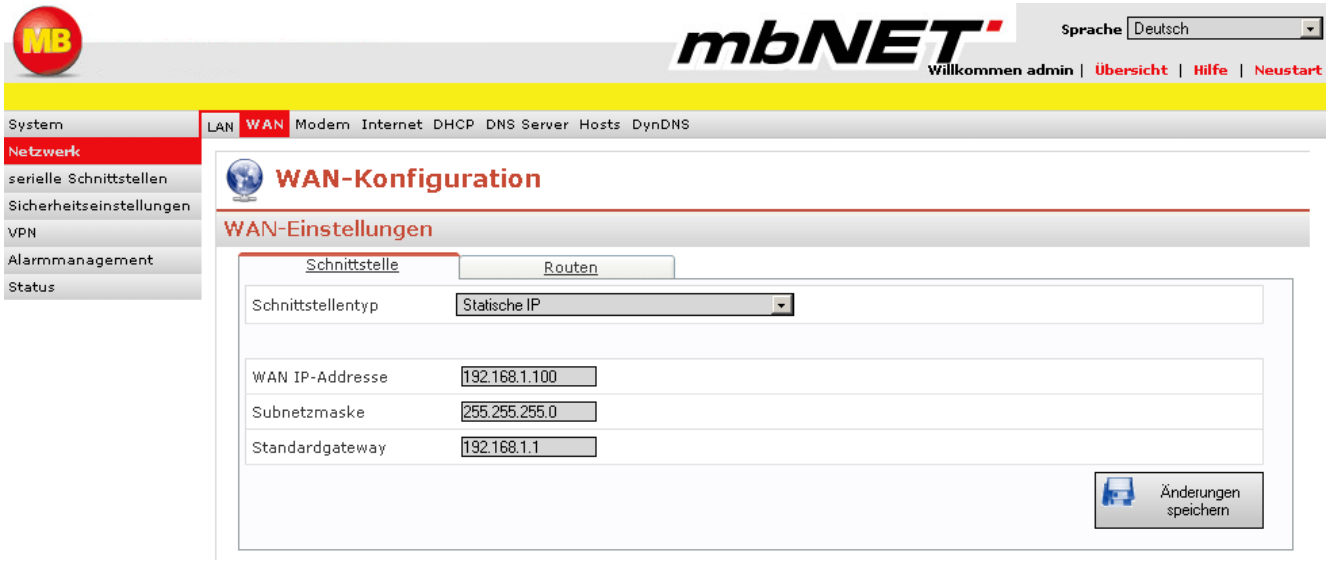


Abbildung 83

Ausführliche Beschreibung der Einstellungen Netzwerk – WAN entnehmen Sie bitte dem Kapitel *Netzwerk - WAN*

Pos.	Bezeichnung	Beschreibung
1	**Schnittstellentyp**	Wählen Sie im Beispiel **Statische IP.** Wenn diese Einstellung gewählt wird, muss ebenfalls ein DNS-Server eingetragen werden (siehe Kapitel **Netzwerk - DNS-Server**).
2	**WAN IP-Adresse**	Geben Sie hier die IP-Adresse des *mbNET* am WAN-Anschluss ein. Hier im Beispiel: 192.168.1.100
3	**Subnetzmaske**	Geben Sie die Subnetzmaske ein. Hier: 255.255.255.0
4	**Standardgateway**	Geben Sie hier den entsprechenden Gateway ein, der Sie mit dem Internet verbindet, also die IP-Adresse des bestehenden Routers. Hier: 192.168.1.1

Konfiguration des Routers bei bestehendem Router für eine Verbindung ins Internet

- ❑ Betätigen Sie ausgehend von der Startseite der Konfigurationsoberfläche die Schaltflächen **Netzwerk – Internet**.

- ❑ Es wird die nachfolgende Bildschirmmaske angezeigt.
  Gehen Sie entsprechend den Beschreibungen auf den nachfolgenden Seiten vor.

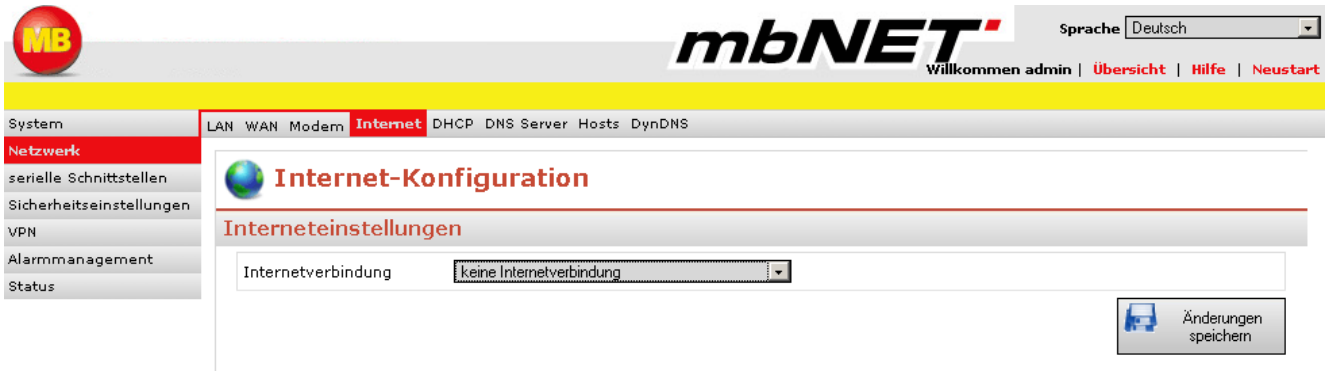


Abbildung 84

Ausführliche Beschreibung der Einstellungen Netzwerk – Internet entnehmen Sie bitte dem Kapitel *Netzwerk - Internet*

Pos.	Bezeichnung	Beschreibung
1	**Internetverbindung**	Wählen Sie im Auswahlfeld die Option **Keine Internetverbindung** aus, da die Internetverbindung durch den bereits bestehenden Router durchgeführt werden soll.

Diese Option heisst „Keine Internetverbindung“ weil das mbNET nicht selbstständig die Verbindung zum Internet aufbaut

- ❑ Speichern Sie die Änderungen durch Anklicken der Schaltfläche **Änderungen speichern.**
- ❑ Um Ihre Änderungen dauerhaft auf dem Industrierouter zu speichern, klicken Sie zum Schluss auf die Schaltfläche **Änderungen übernehmen.**

Abbildung 85

Nachdem sie die Änderungen übernommen haben, bitte den Router neu starten!!!

9.6 Konfiguration des Industrierouters für eine VPN-Verbindung mit einem Client

Um Kosten einer Festverbindung zwischen zwei oder mehreren örtlich voneinander getrennten Netzwerken (LANs) einzusparen und um eine gesicherte Datenübertragung über das unsichere Internet zu gewährleisten, richtet man ein virtuelles Netzwerk ein. Dazu wird mit einem Tunneling-Protokoll eine verschlüsselte Verbindung der sog. VPN-Tunnel aufgebaut.
Bei den in 9.3 und 9.4 beschriebenen Verbindungsszenarien kann ein Client immer nur auf die seriellen Schnittstellen (Beschreibung serielle Schnittstellen siehe Kapitel **Serielle Schnittstellen**) des Routers zugreifen. Ein Zugriff auf die lokale Schnittstelle (LAN) über das Internet war hierbei nicht möglich. Über eine VPN-Verbindung ist es nun möglich an der LAN-Schnittstelle angeschlossene Teilnehmer wie Panel-PC usw. zu erreichen bzw. auf diese zuzugreifen.

Die nachfolgende Abbildung zeigt das Schema einer VPN-Verbindung. Der Client kann z.B. ein PC oder auch ein weiterer Industrierouter sein, der für den Internetzugang entsprechend vorkonfiguriert werden muss.

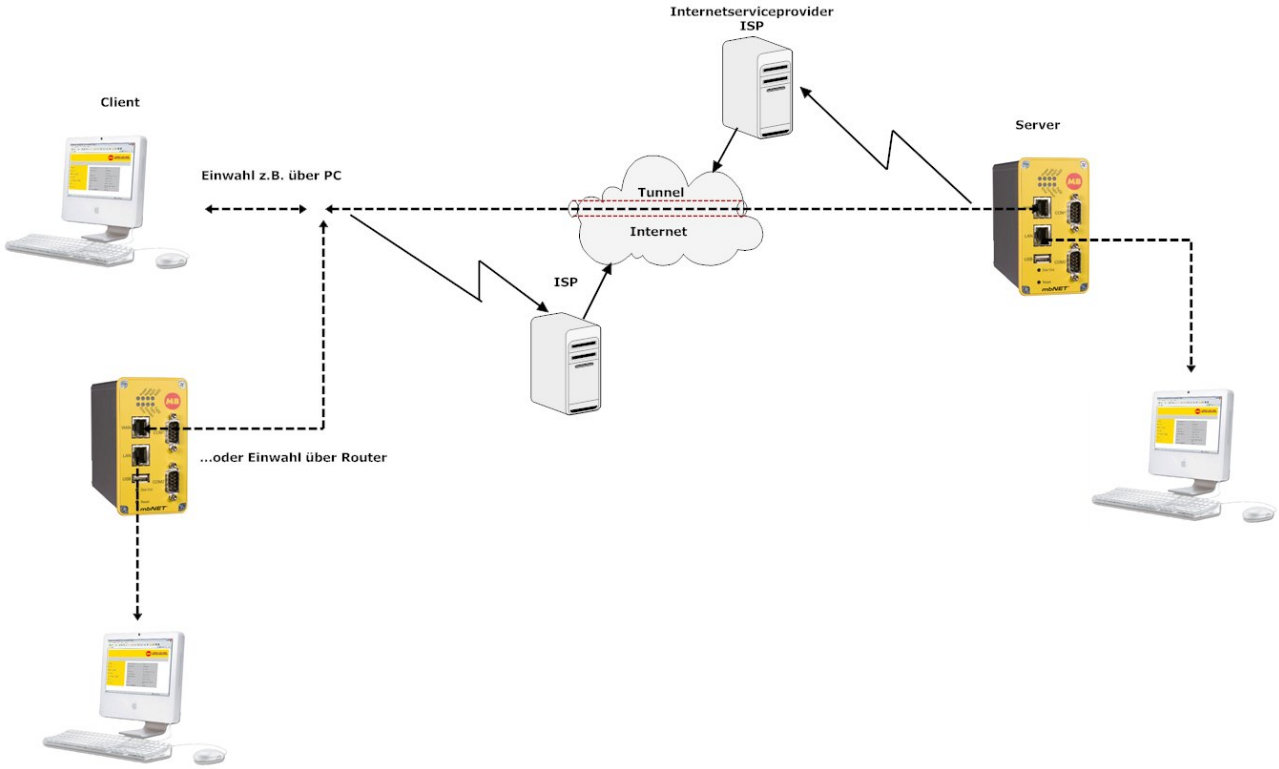


Abbildung 86

Konfiguration des Routers für eine VPN-Verbindung mit einem Client

9.6.1 Anschluss und Konfiguration des Routers

9.6.1.1 Anschluss des Routers

Voraussetzung für eine VPN-Verbindung ist, dass der Router eine Internetverbindung besitzt. Die Vorgehensweise wie man den Router für eine Internetverbindung konfiguriert können Sie abhängig von der Verbindungsart den bereits beschriebenen Verbindungsszenarien entnehmen. Der Router muss grundsätzlich über eine öffentliche IP-Adresse erreichbar sein.

9.6.1.2 Benutzer für VPN-Einwahl anlegen

- Damit sich ein Client per VPN auf den Industrierouter einwählen kann, ist im Benutzermanagement ein Benutzer für VPN-Einwahl anzulegen und diesem das Recht zur VPN-Einwahl zu erteilen. Die genaue Vorgehensweise zum Anlegen eines Benutzers mit bestimmten Rechten entnehmen Sie bitte dem Kapitel ***System – Benutzer***.

IPSEC und PPTP

Als Tunneling-Protokoll stehen bei einer VPN-Verbindung die Protokolle PPTP und IPSec zur Auswahl. Das nachfolgende Beispiel zeigt die Konfiguration einer VPN-Verbindung per PPTP.

Konfiguration des Routers für eine VPN-Verbindung mit einem Client

9.6.1.3 Konfiguration des Routers (VPN-Server)

- ❑ Ausgehend von der Startseite klicken Sie in der linken Navigationsleiste auf **VPN** und in der oberen Navigationsleiste auf **PPTP**.

- ❑ Anhand des folgenden Beispiels soll die Konfiguration deutlich gemacht werden. Nachfolgend die Beschreibung der verschiedenen Konfigurationseinstellungen.

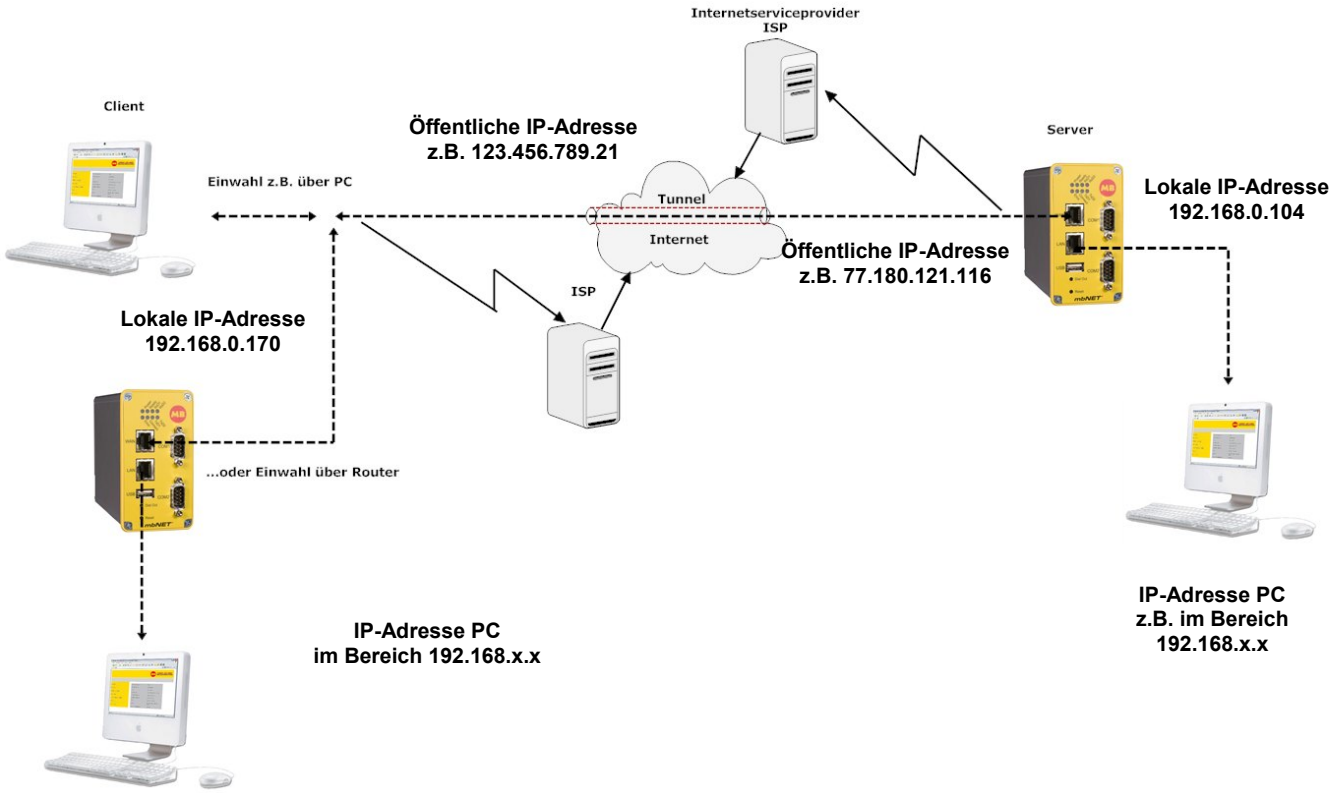


Abbildung 87

- ❑ **Mit dem Verbindungs Assistent** können Sie ihre Verbindungen schnell und einfach konfigurieren. Klicken Sie dazu rechts oben auf den Link Assistenten. Wenn Sie die Funktion des automatischen Öffnens des Assistenten deaktiviert haben, dann klicken Sie auf den Start-Knopf des Assistenten für VPN-Verbindungen. Ansonsten setzen Sie ein Häkchen bei „VPN – Einen VPN-Tunnel einrichten“ und entfernen alle anderen Häkchen.

  Wichtig: Falls Sie ihre Internetverbindung manuell konfiguriert haben, dann wird der VPN-Assistent eine Warnung anzeigen. Wenn Sie noch keine Verbindung zum Internet auf dem mbNET eingerichtet haben, dann beenden Sie bitte den VPN-Assistenten und richten erst eine Internetverbindung ein. Andernfalls setzen Sie ein Häkchen in der Box und klicken auf „Weiter“.
  Bitte beachten Sie auch, dass ab der Firmware 2.0 Sie bei der Webseite des Assistenten zuerst IPSec unter dem Startknopf des VPN-Assistenten auswählen, Änderungen speichern und danach Änderungen übernehmen drücken müssen, damit die Konfiguration für IPSec möglich wird!

- Wählen Sie hier die Option „Verbindung zwischen einem Client-PC und dem mbNET“ und klicken Sie auf „Weiter“.
- Tippen Sie ihren Schlüssel ein (PSK) und klicken Sie auf „Weiter“. Beachten Sie dabei, dass Sie keine Sonderzeichen verwenden sollten und ihr Client diesen Schlüssel auf einem sicheren Weg erhalten muss!
- Nun können Sie eine schon vorkonfigurierte Windows VPN-Verbindung für den Computer vom mbNET herunterladen.

- Für eine manuelle Konfiguration gehen Sie bitte wie folgt vor:

  Ausgehend von der Startseite klicken Sie in der linken Navigationsleiste auf **VPN** und in der oberen Navigationsleiste auf **PPTP** Anschließend auf die Registerkarte ***Server.***

Abbildung 88

- Es erscheint daraufhin die nachfolgende Bildschirmmaske.

Konfiguration des Routers für eine VPN-Verbindung mit einem Client

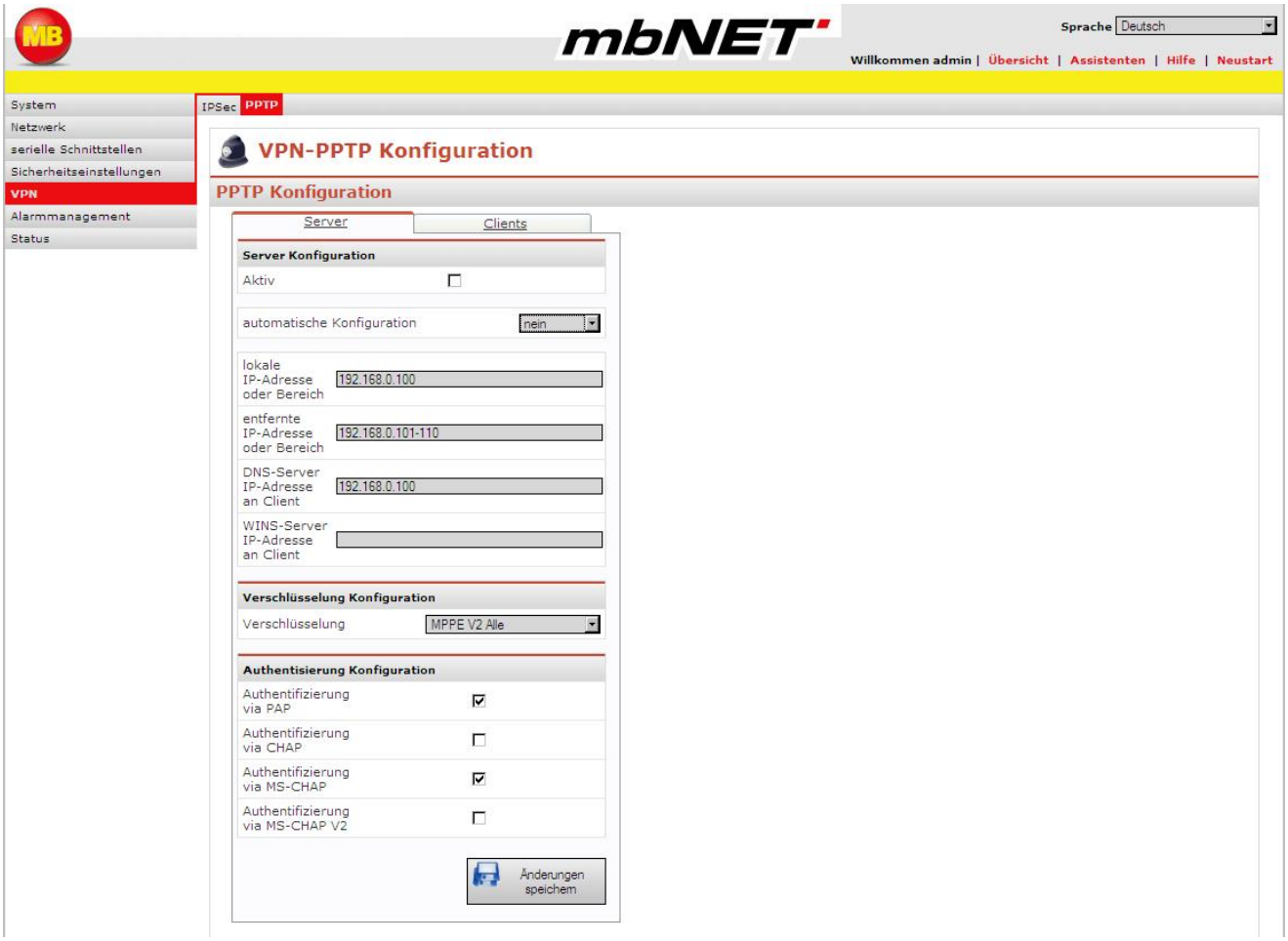


Abbildung 89

Ausführliche Beschreibung der Einstellungen VPN – PPTP entnehmen Sie bitte dem Kapitel *VPN - PPTP*

Bezeichnung	Beschreibung
Aktiv	Versehen Sie die Checkbox durch Anklicken mit einem Häkchen um die Verbindung zu aktivieren.
Automatische Konfiguration	Wenn Sie hier „ja“ wählen, dann wird der PPTP-Server mit der LAN-Adresse des mbNET konfiguriert. Diese Einstellung sollte zuerst ausprobiert werden. Erst wenn es zu Adresskonflikten kommt, sollten Sie Ihre PPTP-Server-Einstellungen händisch eintragen.
Lokale IP Adresse oder Bereich	Tragen Sie in das Eingabefeld eine beliebige lokale Adresse ein. Im Beispiel gewählt: 192.168.10.100 Anmerkung: Sie können auch die LAN-IP des Routers verwenden. Nur bei Adresskonflikten sollten sie den PPTP-Server in einen anderen Adressraum heben.
Entfernte IP Adresse oder Bereich	Tragen Sie hier die entfernten Adressen ein. Im Beispiel gewählt: 192.168.10.160-170 Es werden hiermit den angeschlossenen Clients IP-Adressen aus dem Adressbereich 192.168.10.160 – 192.168.10.170 zugewiesen. **Achtung!** Die hier eingetragene Adresse oder der Adressbereich müssen unbedingt im selben Adressraum liegen, wie die oben gewählte lokale IP-Adresse
DNS-Server IP-Adresse an den Client	Geben Sie hier die DNS-Server-Adresse ein. Hier: 192.168.0.100 (IP-Adresse des Routers)
Verschlüsselung	Übernehmen Sie die werksseitige Einstellung (MPPE V2 alle).
Authentisierung	Übernehmen Sie die werksseitige Einstellung (via CHAP und MS-CHAP V2).

- ❑ Speichern Sie die Änderungen durch Anklicken der Schaltfläche **Änderungen speichern.**
- ❑ Um Ihre Änderungen dauerhaft auf dem Industrierouter zu speichern, klicken Sie zum Schluss auf die Schaltfläche **Änderungen übernehmen.**

Abbildung 90

Einrichtung des Routers für eine VPN-Verbindung(Fortsetzung)

9.6.2 Konfiguration eines Client-PCs für eine VPN-Verbindung zum Router

- ❑ Voraussetzung für die Einrichtung ist, dass eine Internetverbindung seitens des Client-PCs eingerichtet ist. Informationen zur Einrichtung eines Client-PCs entnehmen Sie bitte dem Kapitel ***Konfiguration eines Clients (PCs) für den Zugriff auf den Router***

- ❑ Klicken Sie in Windows unter Systemsteuerung auf **Netzwerkverbindungen** und dann auf **Neue Verbindung erstellen.**

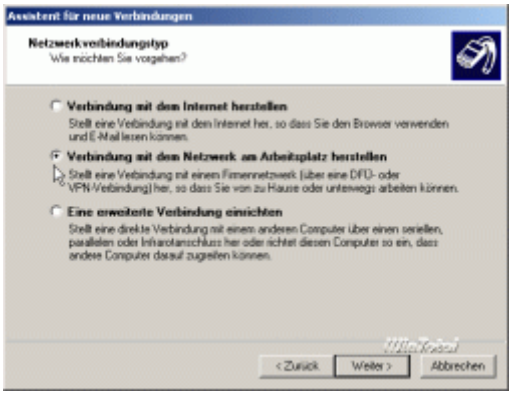

Assistent für neue Verbindungen
Netzwerkverbindungstyp
Wie möchten Sie vorgehen?
Verbindung mit dem Internet herstellen
Stellt eine Verbindung mit dem Internet her, so dass Sie den Browser verwenden und E-Mail lesen können.
Verbindung mit dem Netzwerk am Arbeitsplatz herstellen
Stellt eine Verbindung mit einem Firmennetzwerk (über eine DFÜ- oder VPN-Verbindung) her, so dass Sie von zu Hause oder unterwegs arbeiten können.
Eine erweiterte Verbindung einrichten
Stellt eine direkte Verbindung mit einem anderen Computer über einen seriellen, parallelen oder Infrarotanschluss her oder richtet diesen Computer so ein, dass andere Computer darauf zugreifen können.
< Zurück
Weiter >
Abbrechen

Abbildung 91

- ❑ Wählen Sie beim folgenden Assistenten "**Verbindung mit dem Netzwerk am Arbeitsplatz herstellen.**

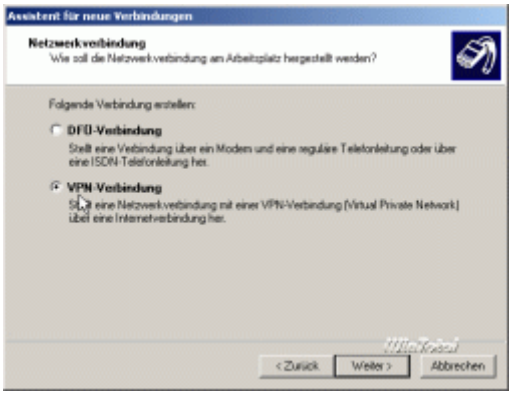

Assistent für neue Verbindungen
Netzwerkverbindung
Wie soll die Netzwerkverbindung am Arbeitsplatz hergestellt werden?
Folgende Verbindung erstellen:
DFÜ-Verbindung
Stellt eine Verbindung über ein Modem und eine reguläre Telefonleitung oder über eine ISDN-Telefonleitung her.
VPN-Verbindung
Stellt eine Netzwerkverbindung mit einer VPN-Verbindung (Virtual Private Network) über eine Internetverbindung her.
< Zurück
Weiter >
Abbrechen

Abbildung 92

- ❑ Im nächsten Dialog wählen Sie **VPN-Verbindung.**

- ❑ Geben Sie jetzt einen Namen für die **VPN-Verbindung** ein.

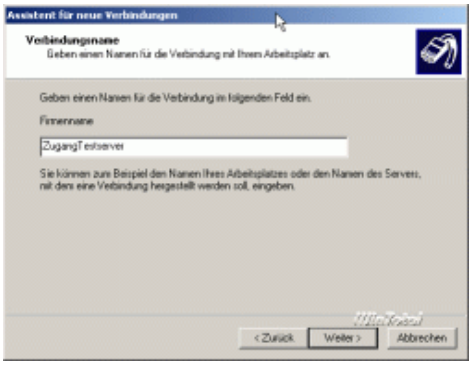

Assistent für neue Verbindungen
Verbindungsname
Geben einen Namen für die Verbindung mit Ihrem Arbeitsplatz an.
Geben einen Namen für die Verbindung in folgendem Feld ein.
Firmenname
ZugangTestserver
Sie können zum Beispiel den Namen Ihres Arbeitsplatzes oder den Namen des Servers, mit dem eine Verbindung hergestellt werden soll, eingeben.
< Zurück
Weiter >
Abbrechen

Abbildung 93

Einrichtung des Routers für eine VPN-Verbindung (Fortsetzung)

Konfiguration eines Client-PCs für eine VPN-Verbindung zum Router (Fortsetzung)

- ❑ Geben Sie hier entweder den Umleitungsnamen des DynDNS-Dienstes an, oder die aktuelle **IP-Adresse** des Routers.

  ► *Als Beispiel wurde die in Abbildung 86 vom Provider zugewiesene IP-Adresse gewählt.*

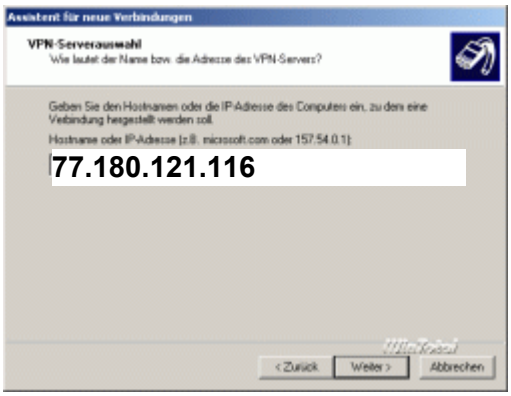


Abbildung 94

Informationen zur Einrichtung und Benutzung des DynDNS-Dienstes von MB Connect Line entnehmen Sie bitte dem Kapitel Netzwerk - DynDNS

Bei Eingabe der IP-Adresse des Routers ist darauf zu achten, dass immer die aktuelle IP-Adresse eingetragen wird (Immer wenn der Router eine Internetverbindung aufbaut, wird ihm eine neue IP-Adresse zugewiesen).

- ❑ Sie können nun auswählen, ob die Verbindung nun für alle, oder nur für den aktuellen Benutzer erstellt werden soll.
- ❑ Erstellen Sie jetzt noch eine Verknüpfung auf dem Desktop.

  ✓ **Die VPN-Verbindung ist jetzt fertig eingerichtet**

Abbildung 95

Einrichtung des Routers für eine VPN-Verbindung(Fortsetzung)

9.6.3 Verbindung zwischen Client-PC und Router über VPN aufbauen

9.6.3.1 Einwahl Router ins Internet

- ❑ Der Router muss abhängig von der Verbindungsart entsprechend für den Internetzugang konfiguriert, im Internet eingewählt und über die IP-Adresse erreichbar sein.

9.6.3.2 Aufbau einer VPN-Verbindung des Clients zum Router

- ❑ Doppelklicken Sie auf das Symbol für die VPN-Verbindung und geben Sie im nachfolgenden Fenster denjenigen Benutzernamen mit Passwort ein, den Sie bei den Routereinstellungen im Benutzermanagement für die VPN-Einwahl die Erlaubnis erteilt haben.

Abbildung 96

9.6.3.3 Weitere Einstellungen

- ❑ Doppelklicken Sie auf das Symbol für die VPN-Verbindung und klicken Sie danach auf Eigenschaften. Unter dem Menüpunkt „Netzwerk“ können Sie den VPN-Typ auf L2TP oder PPTP einstellen. Wählen Sie hier „PPTP-VPN“ aus.

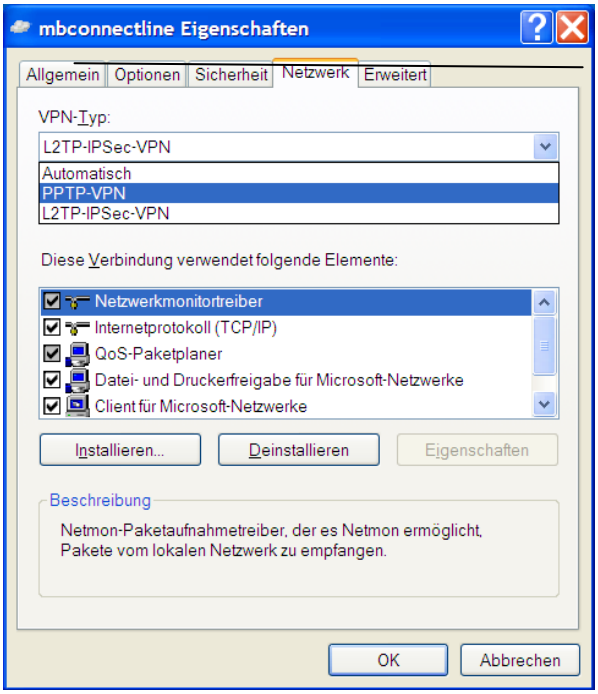


Abbildung 97

Einrichtung des Routers für eine VPN-Verbindung(Fortsetzung)

Eine aktive Verbindung zum Router wird am Client-PC durch ein blinkendes Bildschirmsymbol angezeigt. Durch rechten Mausklick auf das Symbol können Sie sich die Eigenschaften der Verbindung anzeigen lassen.

Über einen PC der mit dem Router verbunden ist, können Sie sich nach Betätigen der Schaltflächen Status in der seitlichen und VPN-PPTP in der oberen Navigationsleiste, über den augenblicklichen Zustand der VPN-Verbindungen wie z.B. momentan auf dem Router eingewählte Benutzer, oder über den aktuellen Verbindungsstatus usw. informieren.

Die Konfigurationseinstellungen eines als Client konfigurierten Industrierouters für den Zugriff auf einen gegenüberliegenden Industrierouter entnehmen Sie bitte dem folgenden Kapitel.

9.7 Konfiguration der Verbindung zwischen zwei Industrieroutern per VPN-PPTP

- Statt eines Client-PCs kann z.B. auch ein weiterer Router als Client konfiguriert werden. Ein Router muss als Client, der andere gegenüberliegende Router als VPN-Server konfiguriert werden. Bei beiden Routern muss eine Internetverbindung eingerichtet sein. Die Konfiguration des Industrierouters als VPN-Server entnehmen Sie bitte dem vorherigen Kapitel ***Konfiguration des Industrierouters für eine VPN-Verbindung mit einem Client***

- Anhand des folgenden Beispiels soll die Konfiguration deutlich gemacht werden.

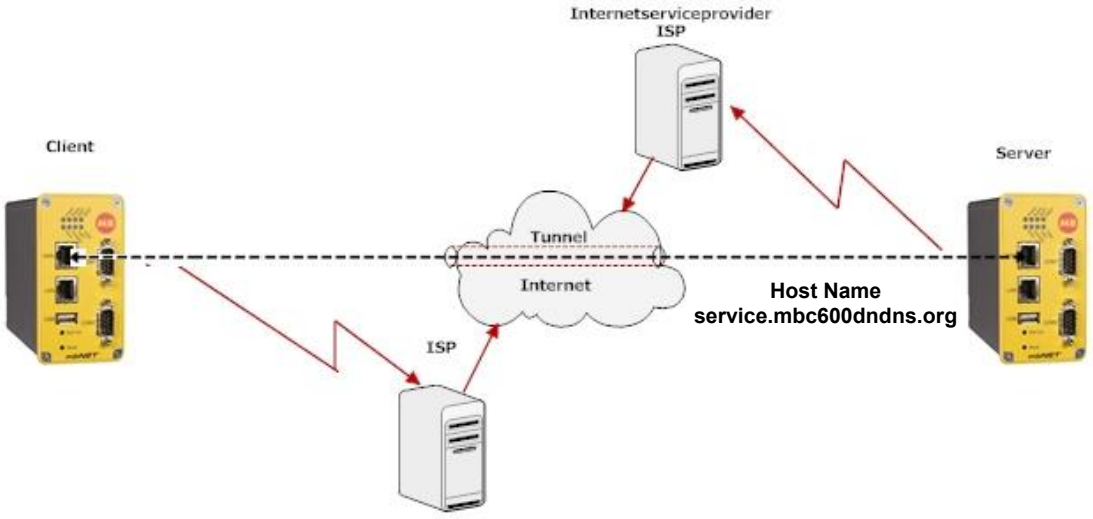


Abbildung 98

9.7.1 Einstellungen für eine Verbindung zwischen zwei Industrieroutern - PPTP-Server

- ☐ Ausgehend von der Startseite klicken Sie in der linken Navigationsleiste auf **VPN** und in der oberen Navgationsleiste auf **PPTP**.
- ☐ Es erscheint daraufhin die nachfolgende Bildschirmmaske

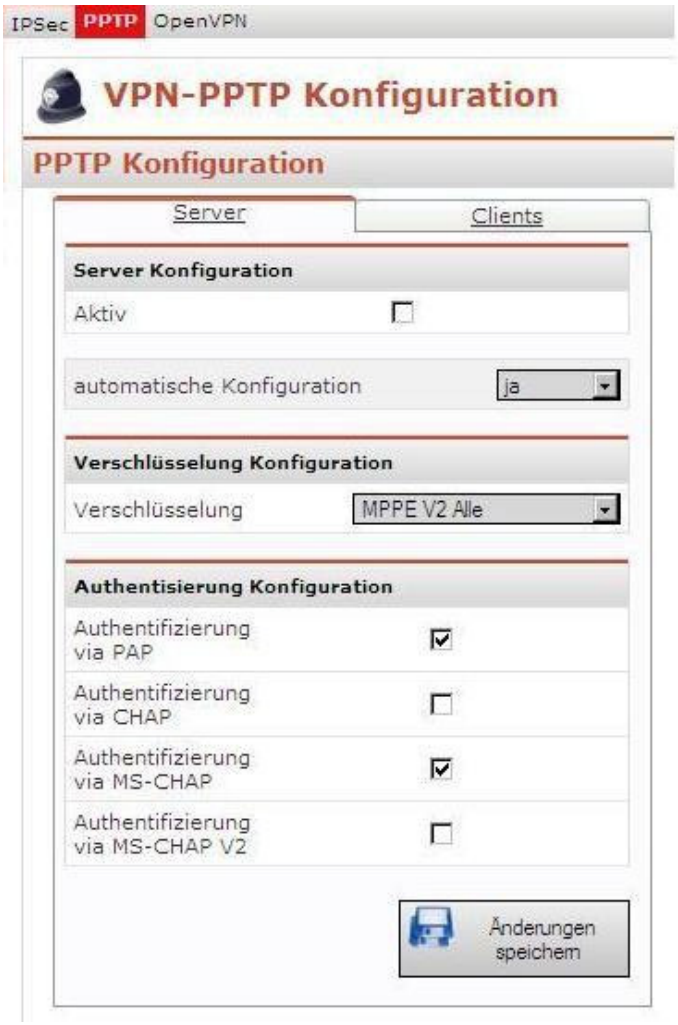


Abbildung 99

Wenn Sie nun den Haken bei Aktiv setzen und diese Einstellung speichern, dann ist ihr Server schon aktiv. Er versorgt die einwählenden Clients dann mit Adressen aus seinem lokalen Netzwerk und der Server nimmt seine LAN-Adresse als PPTP-Serveradresse.

Wenn Sie andere Adressen wünschen, dann stellen Sie die Option „automatische Konfiguration auf NEIN und Sie sehen folgendes Bild:

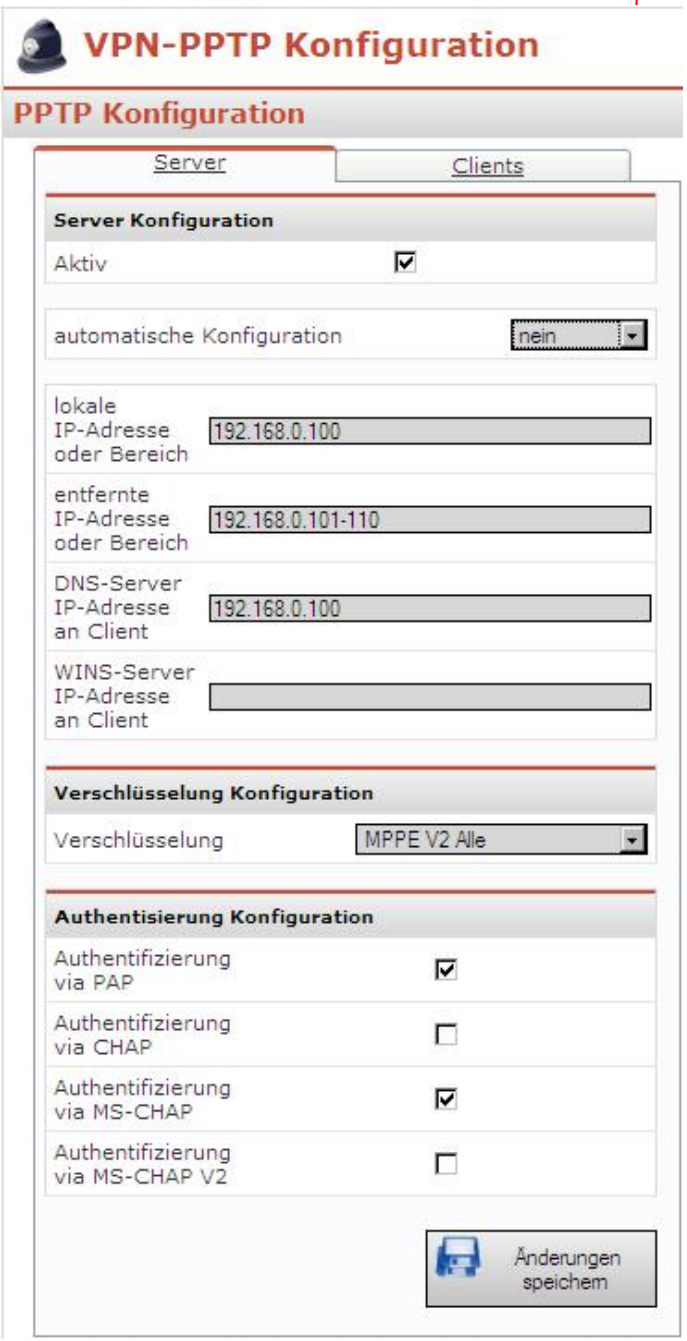


Abbildung 100

Bezeichnung	Beschreibung
Aktiv	Versehen Sie die Checkbox durch Anklicken mit einem Häkchen um die Verbindung zu aktivieren.
Automatische. Konfiguration.	Mit der Möglichkeit „Ja“ wird der lokale Netzbereich und die lokale IP-Adresse des mbNET verwendet. Mit „Nein“ können Sie diese Informationen selbst vorgeben
Lokale IP-Adresse oder Bereich	Hier steht die Adresse des PPTP-Servers
Entfernte IP-Adresse oder Bereich	Tragen Sie hier die Adresse bzw. den Adressbereich für die einwählenden Clients aus.

DNS Serveradresse	Geben Sie hier die Adresse des Servers an, der für die Namensauflösung zuständig ist. Im Standardfall können Sie hier die Adresse des PPTP-Servers eintragen.
WINS-Server IP-Adressee	Zur Kompatibiltät für ältere Microsoft Betriebssysteme kann hier noch die Adresse des WINS-Server angegeben werden.
Verschlüsselung	Mit dieser Option kann die Verschlüsselung der Daten gewählt werden. ☐ MPPE V2 alle ☐ MPPE V2 128 ☐ MPPE V2 40 ☐ Keine **Bitte verwenden Sie die Option „Keine“ nur zu Testzwecken!! Da die gesendeten Daten nicht verschlüsselt werden!!!**
Authentifizierung via PAP, CHAP, MS-CHAP, MS-CHAP V2	Hier können Sie auswählen, welche Authentifizierungsmethoden ihr PPTP-Server unterstützen soll. Setzen Sie die Haken hinter der gewünschten Methode und drücken auf „Änderungen speichern“. Beachten Sie hierbei, dass der Client dann auch die dementsprechende Authentifizierungsmethode nutzen muss, sonst kommt eine Verbindung nicht zustande!

Beachten Sie, dass bei der Verschlüsselung MPPE zum reibungslosen Ablauf I M M E R die Authentifizierungmethode MS-CHAP oder MS CHAP V2 ausgewählt werden muss**.**

Weitere Beschreibung zu VPN – PPTP entnehmen Sie bitte dem Kapitel *VPN - PPTP*

9.7.2 Einstellungen für eine Verbindung zwischen zwei Industrieroutern - PPTP-Client

Abbildung 101

Drücken Sie auf das grüne Plus ganz rechts und es öffnet sich folgende Konfigurationsmaske.

- ☐ Tragen Sie hier einen frei wählbaren Namen für die Verbindung ein.
- ☐ Als nächstes müssen Sie die öffentliche Adresse oder den DynDNS-Namen des PPTP-Servers angeben.
- ☐ Unter dem Punkt „Lokale IP“ kann die Adresse des PPTP-Servers angegeben werden. In der Regel ist dieses Feld freizulassen, da der PPTP-Server beim Verbindungsaufbau seine Adresse sendet.
- ☐ Bei „entfernte IP“ können Sie eine einzelne Adresse angeben, oder ein ganzes Netz. Wir empfehlen die Einstellung wie in der Abbildung 102 vorzunehmen und eine Netzadresse vorzugeben. Hiermit ist dann möglich, auf alle Teilnehmer dieses Netzes zu zugreifen. **Bitte beachten Sie, dass die Netzadresse in der CIDR-Schreibweise vorzunehmen ist, wie es die Abbildung 102 zeigt (192.168.0.0/24)**
- ☐ Wählen Sie bei Authentisierung eine Methode die der PPTP-Server unterstützt. Dies können Sie auf dem PPTP-Server auf der Webseite des Servers unter VPN-PPTP nachsehen
- ☐ Benutzen Sie die gleiche Verschlüsselung wie der Server. Bitte beachten Sie, dass bei einer Verschlüsselung mit MPPE immer die Authentifizierungsmethode MS-CHAP oder MS-CHAP V2 aktiviert sein muss!
- ☐ Für die Felder Benutzer und Passwort ist ein Benutzer gefordert, der vorher auf dem PPTP-Server angelegt wurde (Bsp. der Standardbenutzer ADMIN ohne Passwort). Sie können aber auch einen neuen Benutzer auf dem Server anlegen (Dazu müssen Sie auf die Weboberfläche des Servers unter System-Benutzer wechseln).
- ☐ Als letzte Option können Sie noch wählen auf welches Ereignis sich der Client verbinden soll. Es stehen folgende Möglichkeiten zur Auswahl:
  - Verbindung immer aufrecht erhalten
  - Verbindung bei Datentransfer
  - Bei Signal 1 am digitalen Eingang 1-4

Abbildung 102

- Speichern Sie die Änderungen durch Anklicken der Schaltfläche **Änderungen speichern.**
- Um Ihre Änderungen dauerhaft auf dem Industrierouter zu speichern, klicken Sie zum Schluss auf die Schaltfläche **Änderungen übernehmen.**

Abbildung 103

Weitere Beschreibungen der Einstellungen VPN – PPTP entnehmen Sie bitte dem Kapitel *VPN - PPTP*

Bezeichnung	Beschreibung
Aktiv	Versehen Sie die Checkbox durch Anklicken mit einem Häkchen um die Verbindung zu aktivieren.
Name	Vergeben Sie einen Namen für den Client. Im Beispiel wurde gewählt: nach PPTPclientVerbindung
Hostname oder IP	Tragen Sie hier den Namen oder die IP-Adresse ein, unter der der Client den Server erreicht. Hier als Beispiel: 123456789@mbNET.mymbnet.biz
Lokale IP	Hier kann die Adresse des Servers stehen. In der Regel kann dieses Feld freigelassen werden.
Entfernte IP	Tragen Sie die Adresse der Gegenstelle ein oder die Adresse eines ganzen Netzes. Wir empfehlen die Angabe einer Netzadresse . Im Beispiel: 192.168.0.0/24. Beachten Sie bitte die CIDR-Schreibweise (/24 hinter der Netzadresse)
Authentisierung	Wählen Sie eine Authentifizierungsmethode die auch am Server eingestellt ist.
Verschlüsselung	Es ist empfehlenswert die Verschlüsselungsmethode MPPE V2 alle zu wählen. Beachten Sie, dass wenn Sie die Option „Keine“ verwenden, ihre Daten NICHT verschlüsselt werden.
Benutzer & Passwort	Tragen Sie den Benutzernamen und zugehörige Passwort eines Benutzers ein, der am PPTP-Server unter System-Benutzer eingetragen ist (Bsp. ADMIN ohne Passwort)
Start Verbindung bei	Wählen Sie **Verbindung immer aufrechterhalten**. Beim Neustart oder Bootvorgang wird die Verbindung aufgebaut. Es ist aber auch möglich nur auf bestimmte Ereignisse die Verbindung zu starten.

.

10. Zertifikate und Widerrufslisten erstellen mit XCA

10.1 Überblick Zertifikate

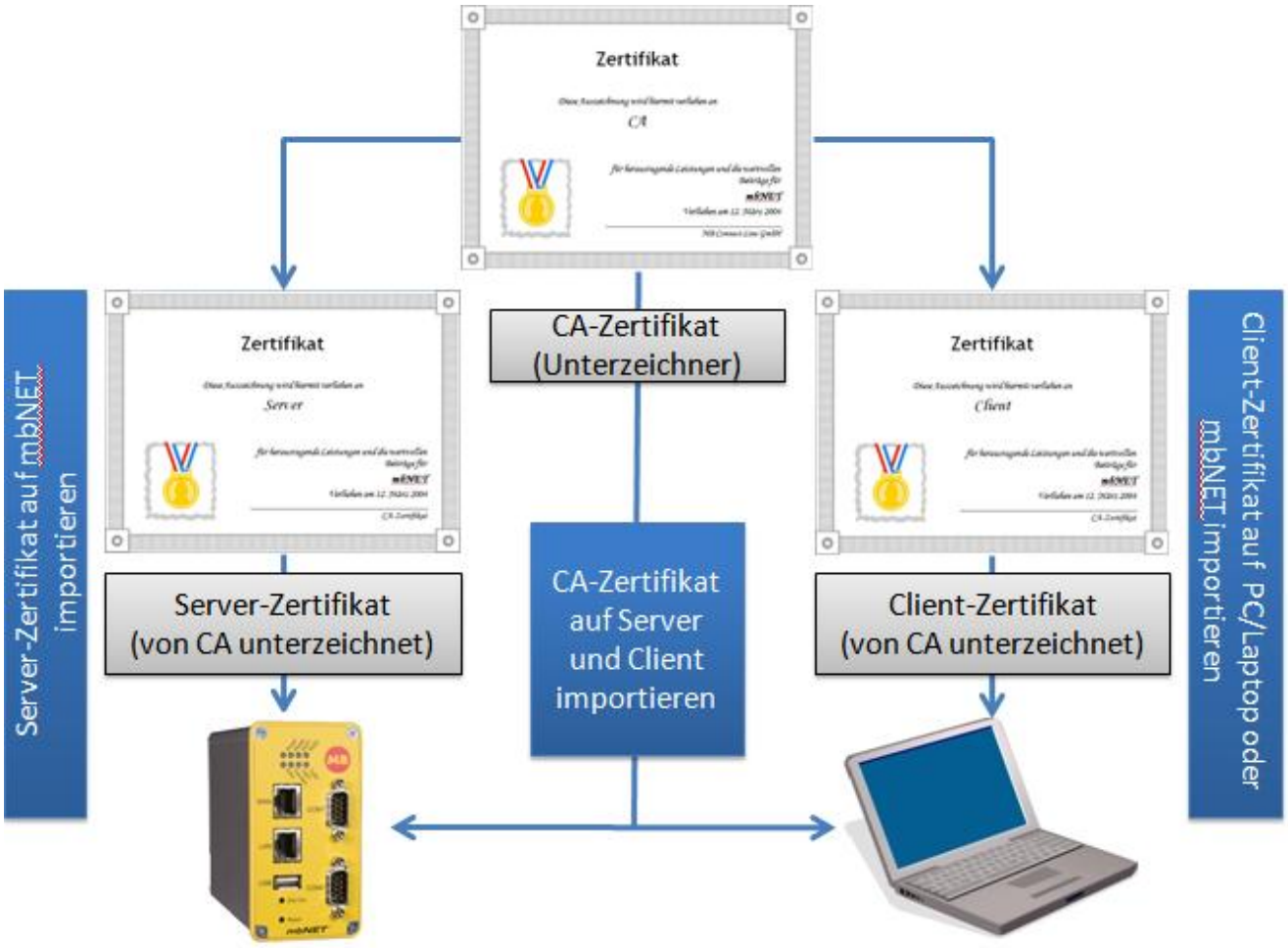


Abbildung 104

Jeder Kommunikationsteilnehmer einer VPN-Verbindung muss 2 Zertifikate besitzen. Ein Zertifikat hat die Eigenschaft, dass es von einem so genannten CA-Zertifikat (Stammzellenzertifikat) unterzeichnet sein muss. Jeder Teilnehmer muss das CA-Zertifikat und zusätzlich noch ein „Server"- bzw. „Client"-Zertifikat besitzen. Server in unserem Falle ist immer das mb*NET*. Client ist entweder ein PC/Laptop oder ein anderes mb*NET*. Die Zertifikate werden benötigt um einen sicheren VPN-Tunnel aufzubauen und dienen zur Authentisierung der VPN-Teilnehmer. Besitzt ein Teilnehmer kein oder ein ungültiges Zertifikat ist zwischen den beiden Geräten kein Aufbau des VPN-Tunnels möglich, wenn die Authentisierung des *mbNET* auf „X.509" eingestellt ist.

Wie Sie Zertifikate erstellen können, entnehmen Sie bitte den folgenden Punkten.

10.2 Erstellen von Zertifikaten

Um Zertifikate erstellen zu können, bietet es sich an, das frei erhältliche Programm XCA von Christian Hohnstädt zu verwenden. Hiermit ist es auf einfache Art und Weise möglich, sowohl X.509- Zertifikate, als auch die benötigten privaten Schlüssel zu erstellen.
Das Programm ist unter http://sourceforge.net/projects/xca kostenlos erhältlich und kann unter Windows wie gewohnt installiert werden (Führen Sie dazu die Datei mit der Endung `.exe` aus).

Wenn man XCA zum ersten Mal startet, muss zunächst eine neue Datenbank erstellt werden, in der die Zertifikate zu verwalten sind. Klicken Sie dazu auf „Datei“ und danach auf „Neue Datenbank“.

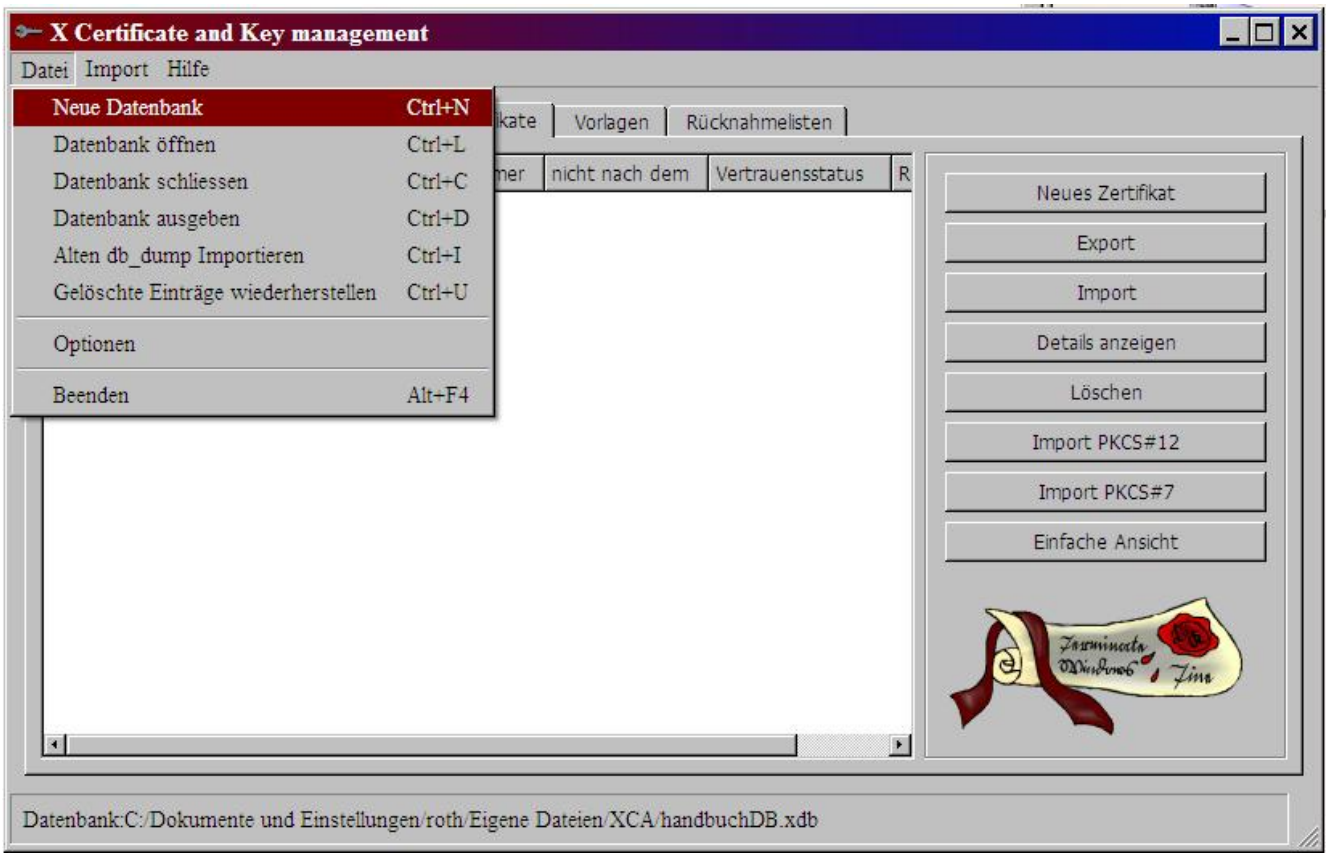


Abbildung 105

Nachdem ein Name, der Speicherort und das Passwort für die Datenbank gewählt wurde, kann die Datenbank geöffnet und damit begonnen werden ein Stammzellenzertifikat (CA-Zertifikat) zu erstellen.

10.2.1 Erstellung eines Stammzellenzertifikats

Um ein Stammzellenzertifikat zu erstellen klicken Sie auf die Registerkarte *„Zertifikate“* und öffnen mit einem Klick auf *„Neues Zertifikat“* die folgende Dialogbox.

10.2.1.1 Stammzertifikat Herkunft

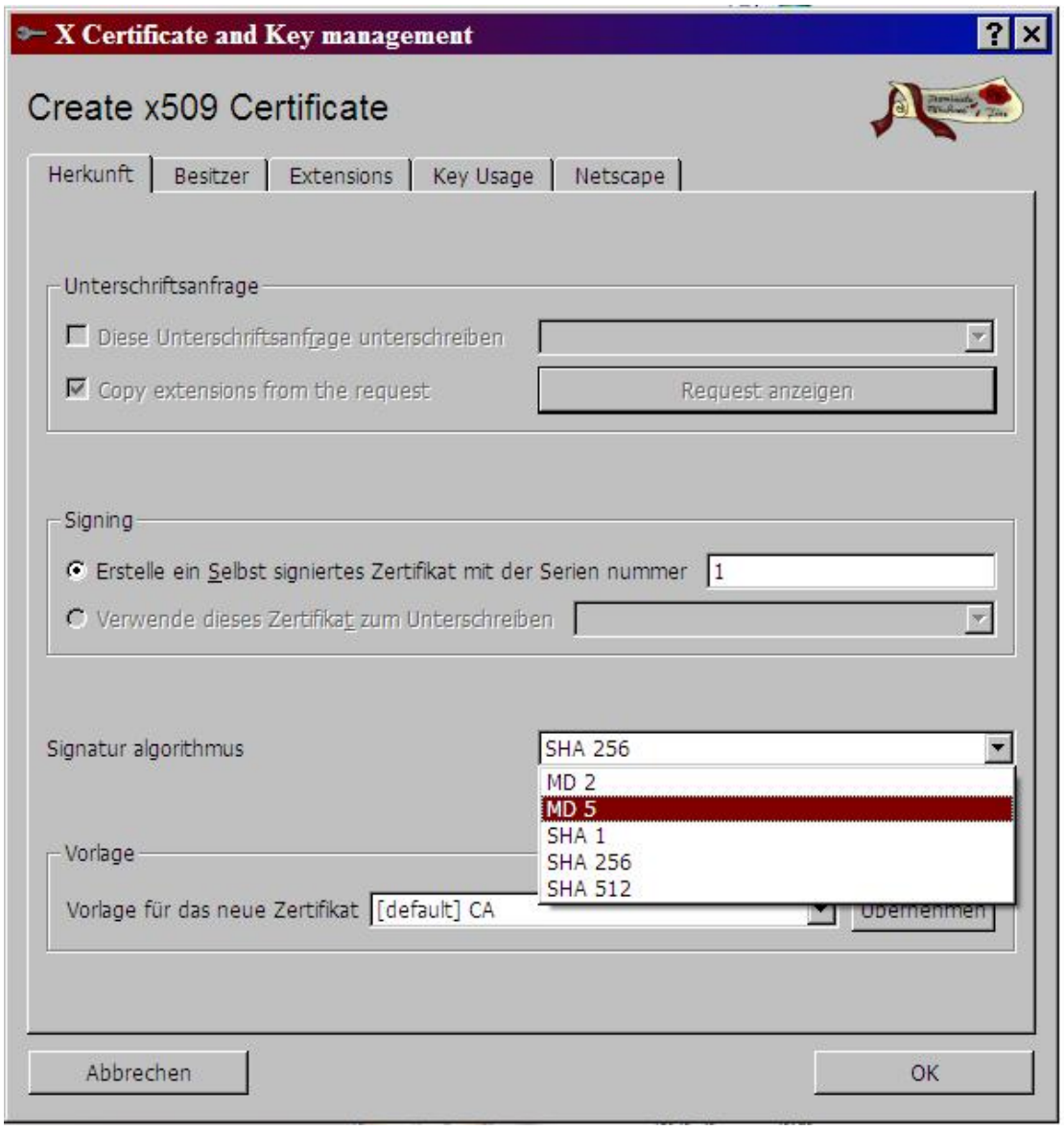


Abbildung 106

Zunächst sollten Sie den Signatur Algorithmus auf MD 5 ändern, damit das Zertifikat mit dem *mbNET* kompatibel wird. Ist dies erledigt, können Sie gleich auf den Reiter *„Besitzer“* wechseln und die Zertifikats-einstellungen vornehmen.

10.2.1.2 Stammzertifikat Besitzer

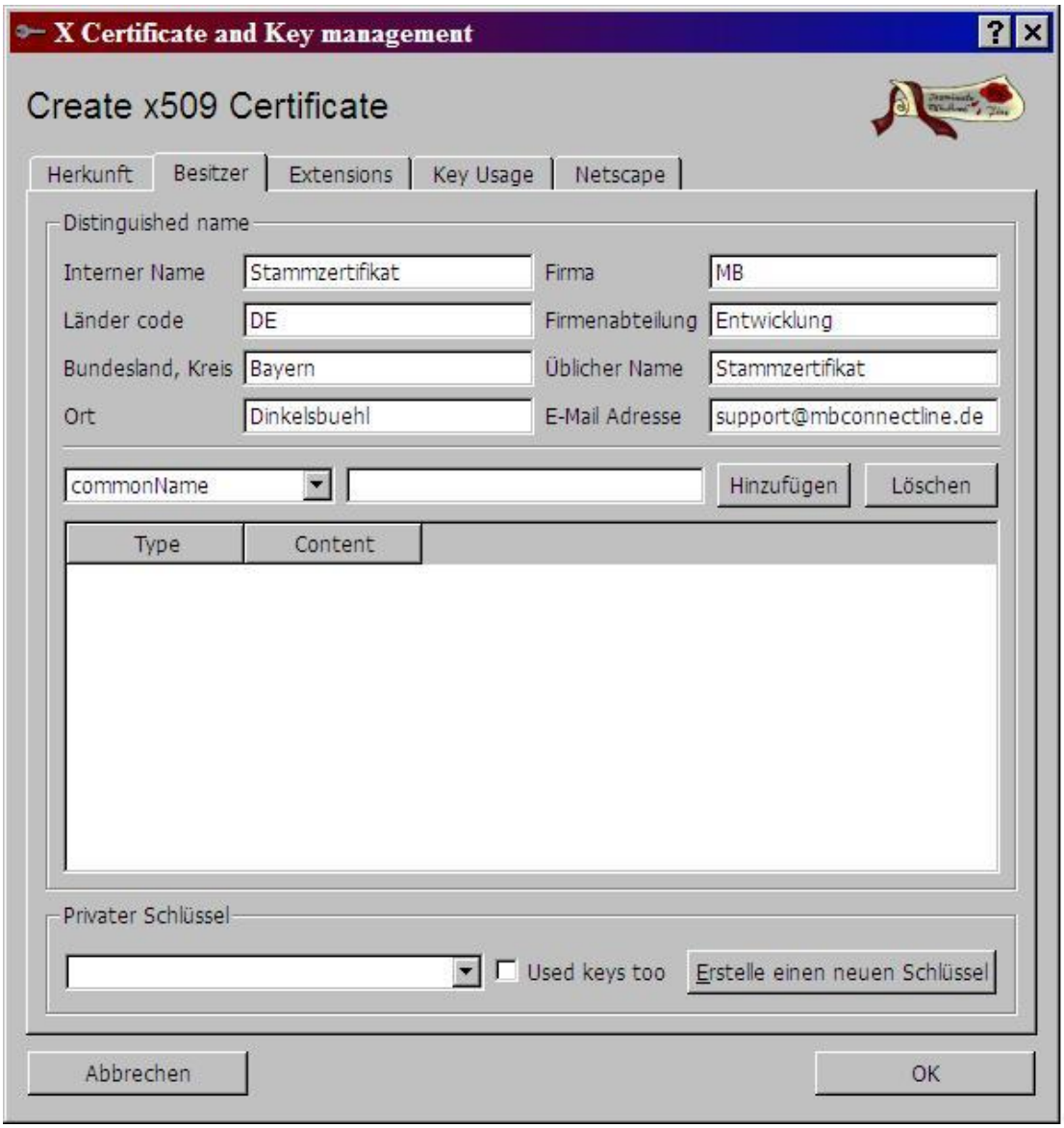


Abbildung 107

Füllen Sie in der Registerkarte *"Besitzer"* die Felder von „Interner Name" bis „E-Mail Adresse" aus. Bei VPN über IPSec können die Besitzereinstellungen später als ID verwendet werden (vgl. Kapitel Authentisierung)
Anschließend muss durch einen Klick auf *„Erstelle einen neuen Schlüssel"* ein privater Schlüssel erstellt werden.

Bitte beachten Sie, dass Umlaute zu vermeiden sind! (Beispiel: bei Ort Dinkelsbuehl)

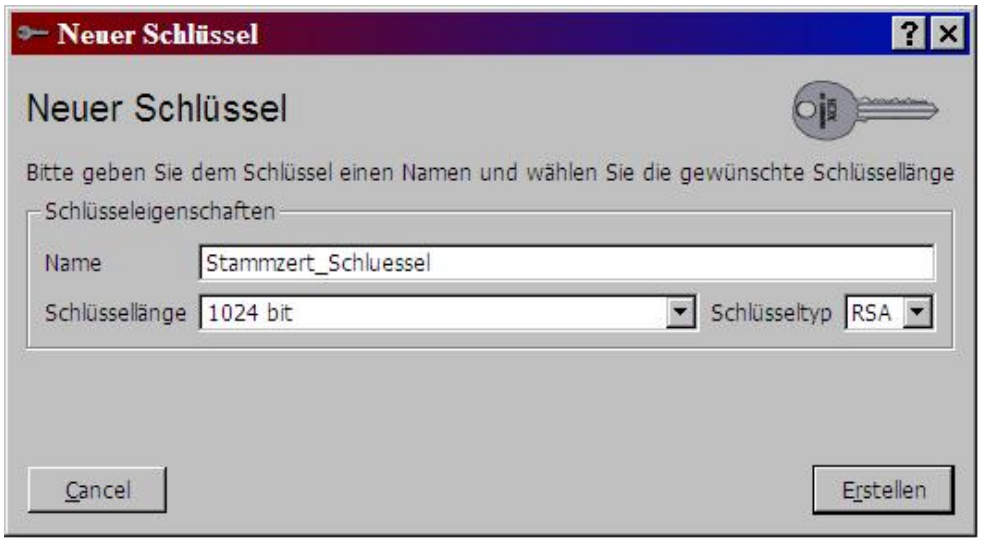


Abbildung 108

Als Schlüsseltyp muss RSA verwendet werden. Die Schlüssellänge und natürlich auch der Name können frei gewählt werden. Je länger der Schlüssel ist, desto sicherer aber auch rechenintensiver wird die Verschlüsselung.

10.2.1.3 Stammzertifikat Extensions

Im Reiter „Extensions“ sind die Einstellungen für Art und Gültigkeit des Zertifikats vorzunehmen.

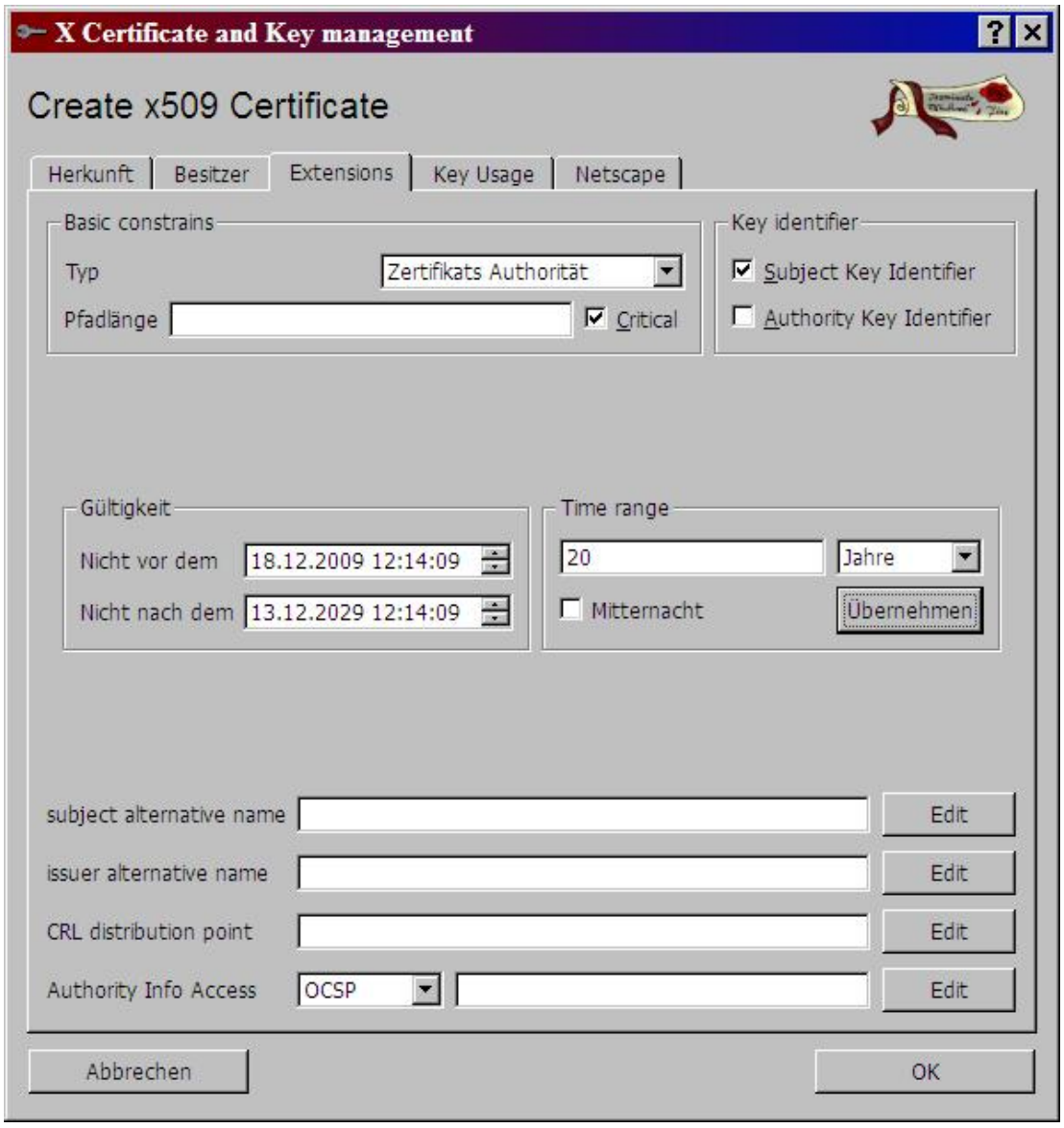


Abbildung 109

Basic constrains
Typ = Zertifikats Authorität (CA)
Haken setzen bei der Option Critical

Key identifier
Haken setzen bei Subject Key Identifier

Gültigkeit
Sie können das genaue Anfangs-/ und Enddatum in die ausgewiesenen Felder eingeben, oder den nebenstehenden Eintrag Time Range benutzen.

Time Range
Stellen Sie im Menü ganz rechts den Zahlenwert Tage, Monate oder Jahre ein. Welche Dauer einzelne Zertifikate haben sollten, sehen Sie in der unten angegebenen Aufstellung:

- Personenzertifikate sollten 1 Jahr Gültigkeit haben.
- Server (SSL) Zertifikate ebenfalls 1 Jahr Gültigkeit.
- Router Zertifikate sollten 1 (wenn es fremde Router sind) oder 10 Jahre (wenn es eigene Router sind) Gültigkeit haben.
- CA Zertifikate sollten auch eine lange Laufzeit haben (Bsp. >10 Jahre).

Bitte mit *„Übernehmen“* die Werte der Einstellmöglichkeiten bei **Time Range** übernehmen

Subject alternative name
Der alternative Name des Inhabers besteht aus einer Liste von alternativen Namen für den Inhaber des Zertifikates, diese Namen können, RFC822-Namen (E-Mail), DNS-Namen, X.400 Adressen, EDI-Namen, URIs oder IP-Adressen sein, im Grunde ist jedes strukturiertes Namenschema verwendbar. Bei PKIX muss diese Erweiterung kritisch sein, wenn das Subject-Feld im Zertifikat leer ist.

Issuer alternative name
Für alternative Namen des Austellers gilt dasselbe wie für den alternativen Namen des Inhabers.

CRL distribution point
Um einen öffentlichen Zugangspunkt für Rückhollisten benutzen zu können, muss die LDAP-/ bzw. HTTP-Adresse der Rückholliste Liste eingetragen werden. Es ist der Adresse immer ein **URI** (universal resource indicator) (z.B. URI:http://de.wikipedia.de) voran zu setzen. Das Feldtrennzeichen ist ein Doppelpunkt. Falls Sie lokale Rückhollisten besitzen, ist diese Option für Sie nicht von Bedeutung.

Authority Info Access
Diese PKIX Erweiterung definiert, wie weitere Information und Services der ausstellenden CA genutzt werden können. Darin können weitere Informationen über die CA (weitere Richtlinien, Stammzertifikate,...) oder Online Verifikation Services (z.B. OCSP) bereitgestellt werden. Vor allem wenn bei Zertifikatsanwendungen wie Secure Mail (S/MIME) nicht der ganze Zertifizierungspfad mitgeschickt wird, ist es für die prüfende Anwendung nett, wenn im Endzertifikat in dieser Erweiterung aufgeführt ist, wo das nächsthöhere CA-Zertifikat abzurufen ist.

10.2.1.4 Stammzertifikat Key Usage

Unter dem Reiter *„Key Usage“* können Sie die Schlüsselauswahl und die erweiterte Schlüsselauswahl treffen. Beide Schlüssel sollten nicht kritisch sein, d.h. Sie sollten keine Haken in die beiden Checkboxen Critical setzen.

Wählen Sie bitte in der linken Spalte folgende Werte aus, wenn Sie ein Stammzellenzertifikat erstellen möchten:

- Certificate Sign
- CRL Sign

Mit diesen beiden Optionen kann mit ihrem Stammzellenzertifikat die Clientzertifikate und die Rückhollisten unterschrieben werden.

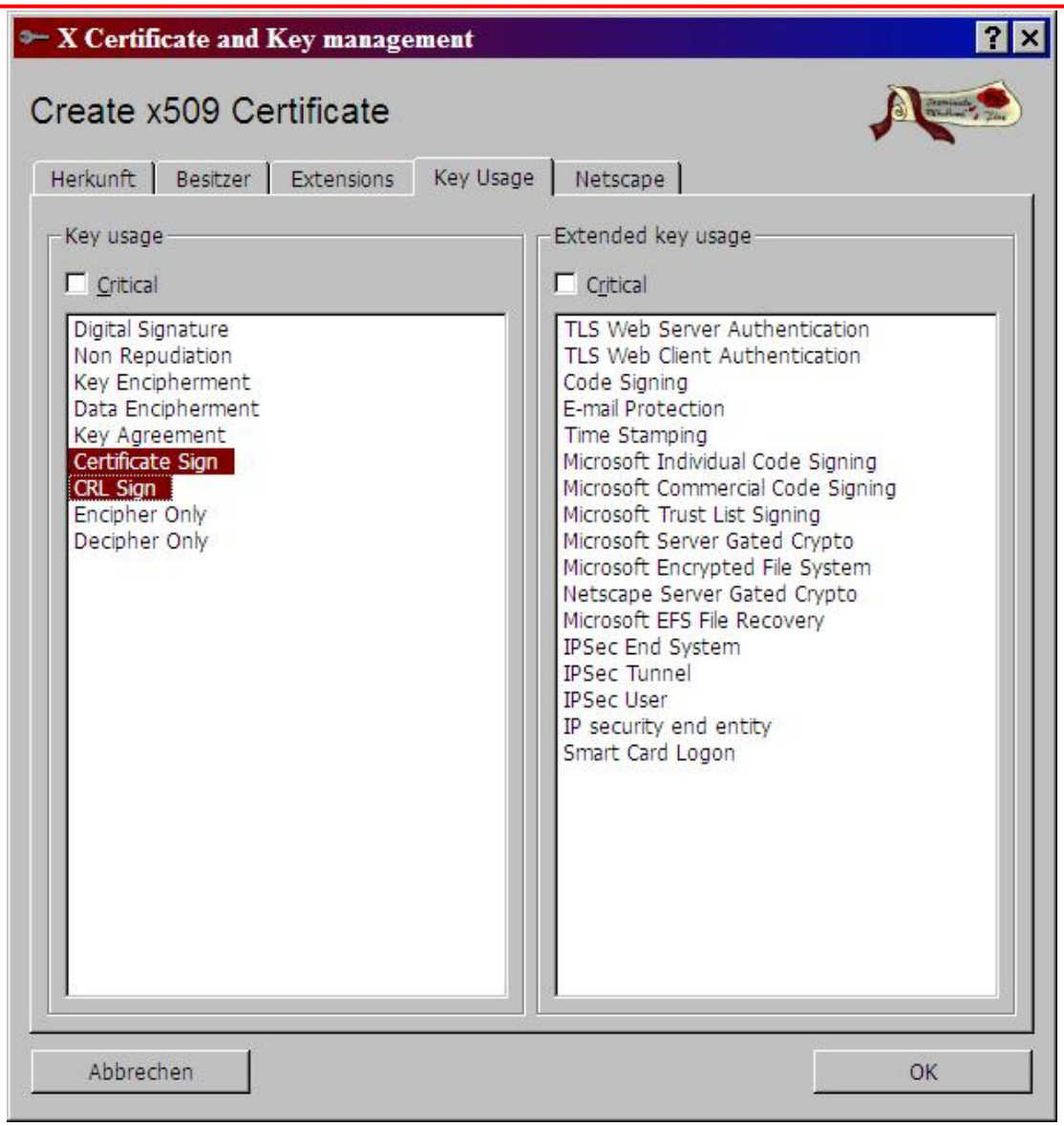


Abbildung 110

Nun können Sie mit einem Klick auf *„OK“* die Erstellung des Stammzellenzertifikats abschließen. Ihr Stammzellenzertifikat ist somit fertiggestellt und Sie können damit ihre weiteren Zertifikate davon ableiten und unterschreiben.

10.2.2 Erstellung eines Clientzertifikats

Um nun ein Zertifikat zu erstellen, welches von dieser CA unterzeichnet ist, markiert man nun im Reiter *„Zertifikate“* das soeben erstellte Stammzertifikat und klick erneut auf *„Neues Zertifikat“*.

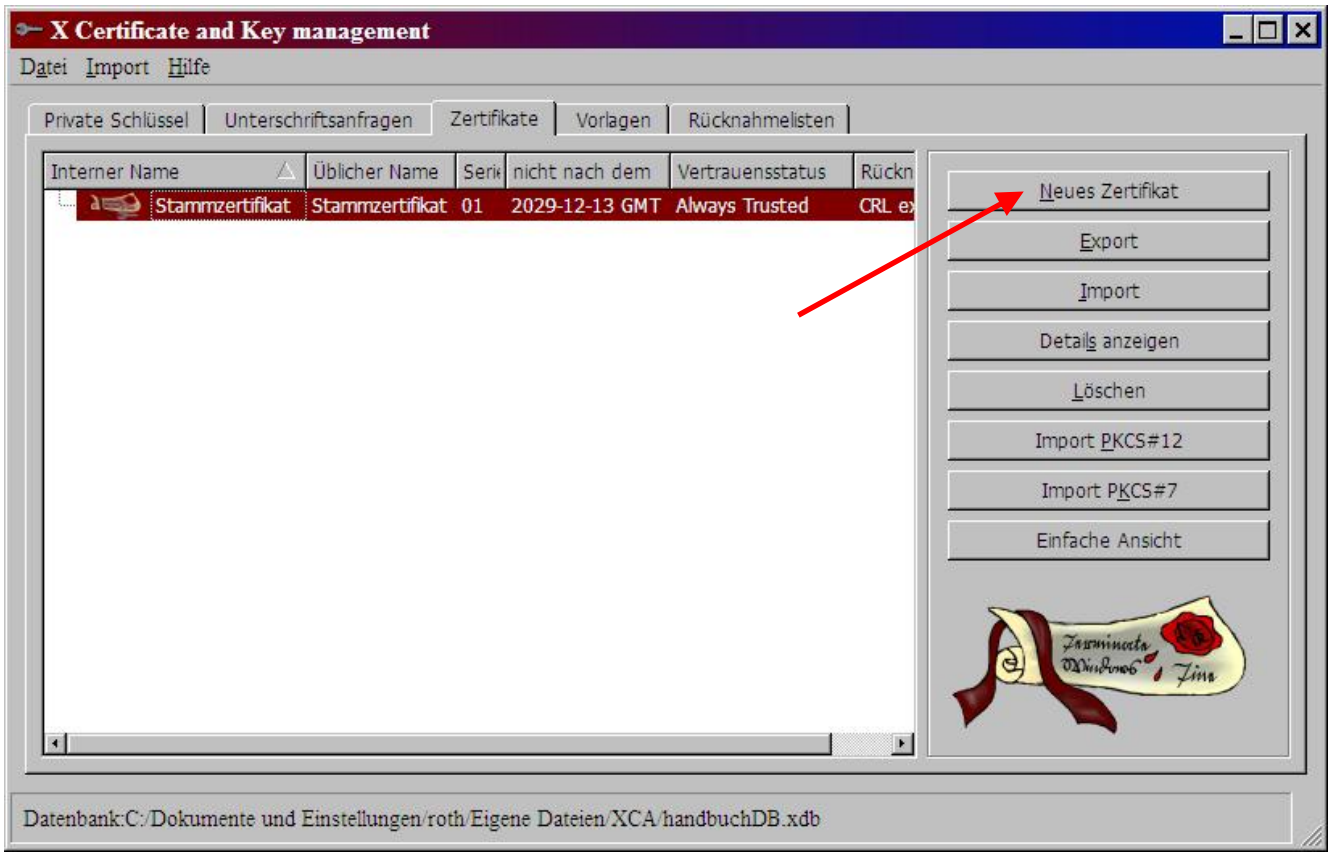


Abbildung 111

Danach erscheint der folgende Dialog.

10.2.2.1 Clientzertifikat - Herkunft

Zunächst müssen wir angeben, dass unser Stammzertifikat zum unterschreiben verwendet werden soll. Auch ist wieder der Signaturalgorithmus MD5 einzustellen

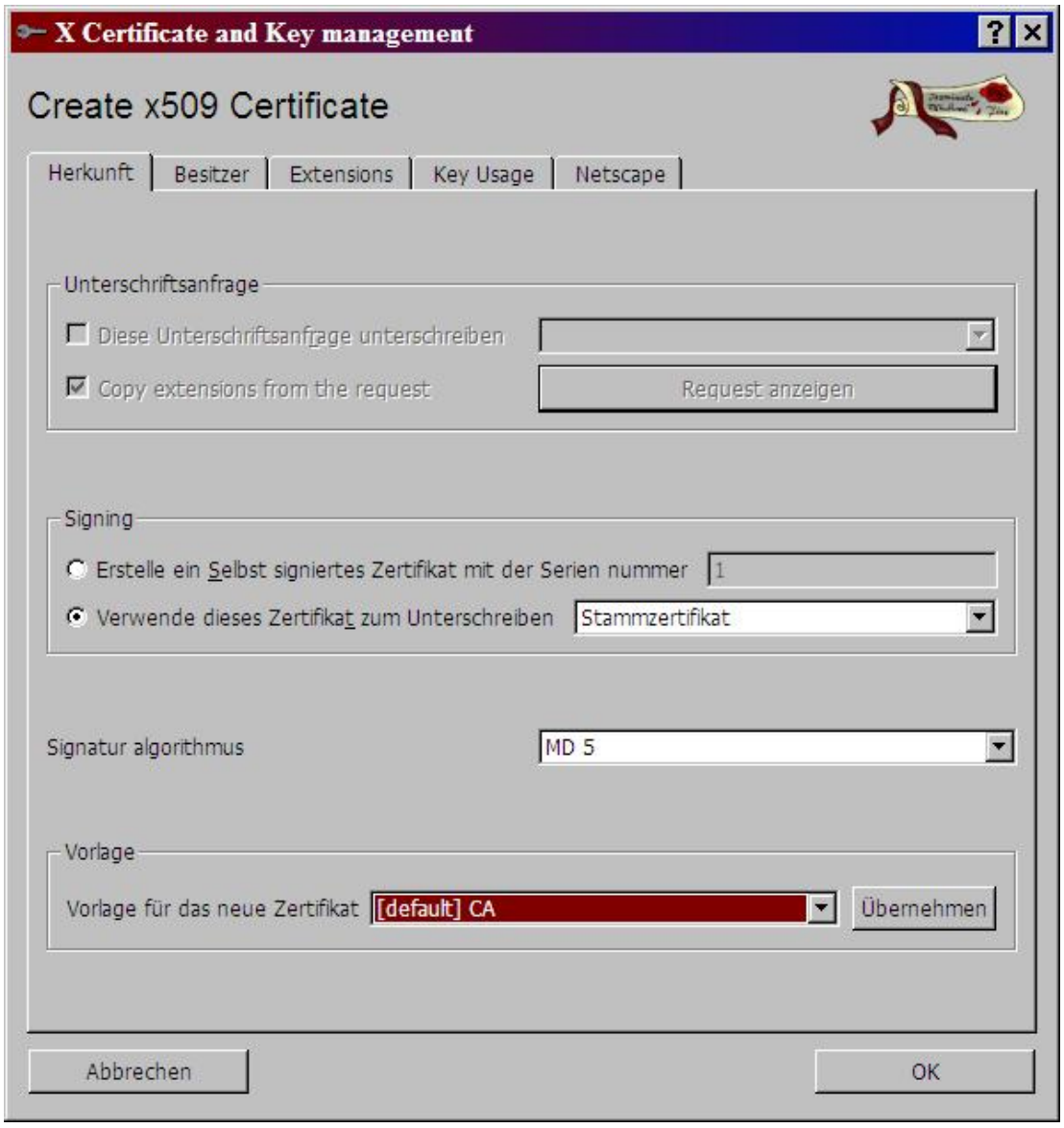


Abbildung 112

Hier ist bereits voreingestellt, dass unser Stammzertifikat zum Signieren verwendet werden soll.

10.2.2.2 Clientzertifikat - Besitzer

Vergeben Sie hier wieder die Daten für das Clientzertifikat von Interner Name bis EMail-Adresse.

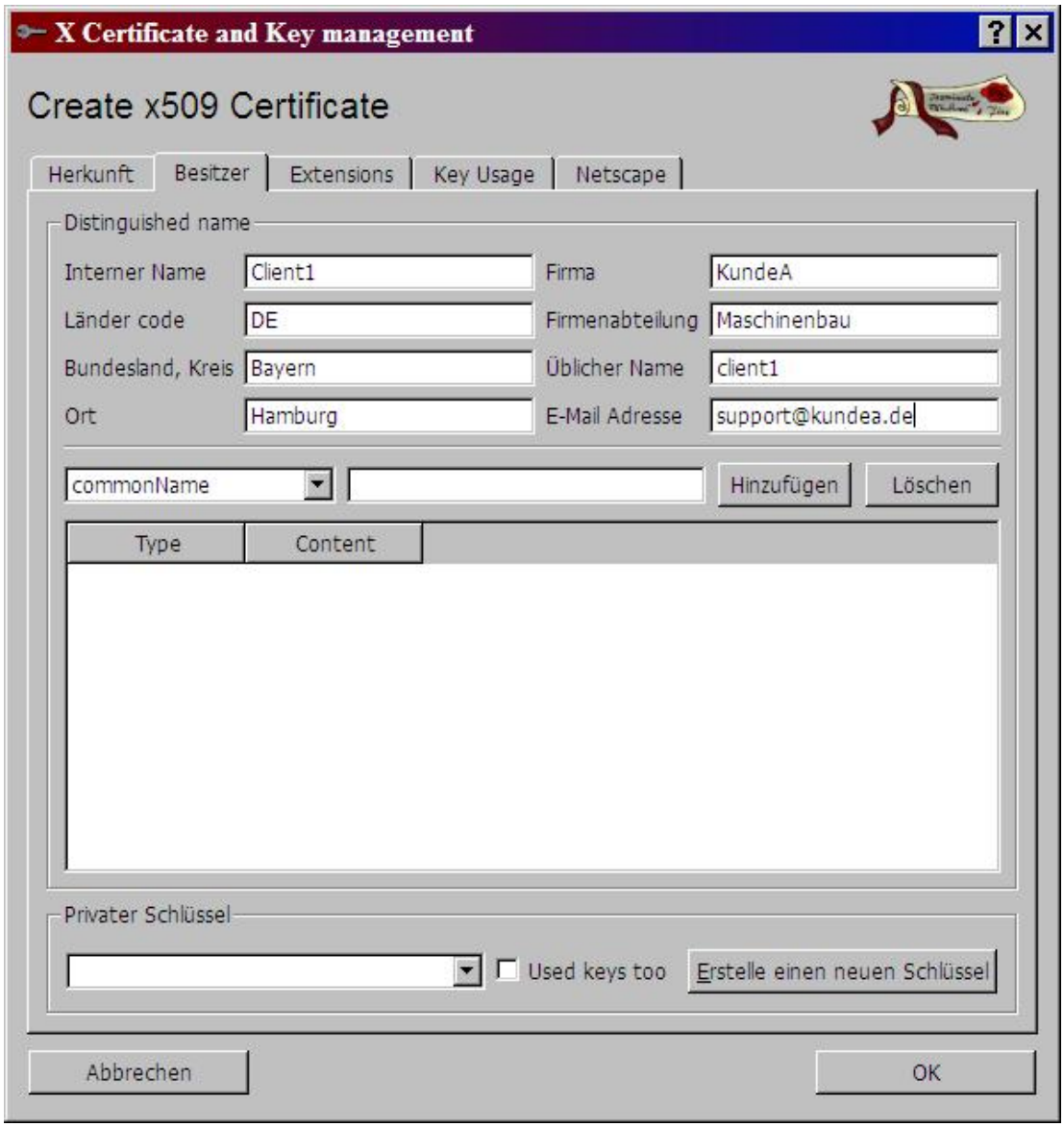


Abbildung 113

Erstellen Sie danach auch einen Schlüssel für das Clientzertifikat. Es ist empfehlenswert das dieser Schlüssel die gleiche Länge hat wie der Schlüssel des Stammzertifikats.

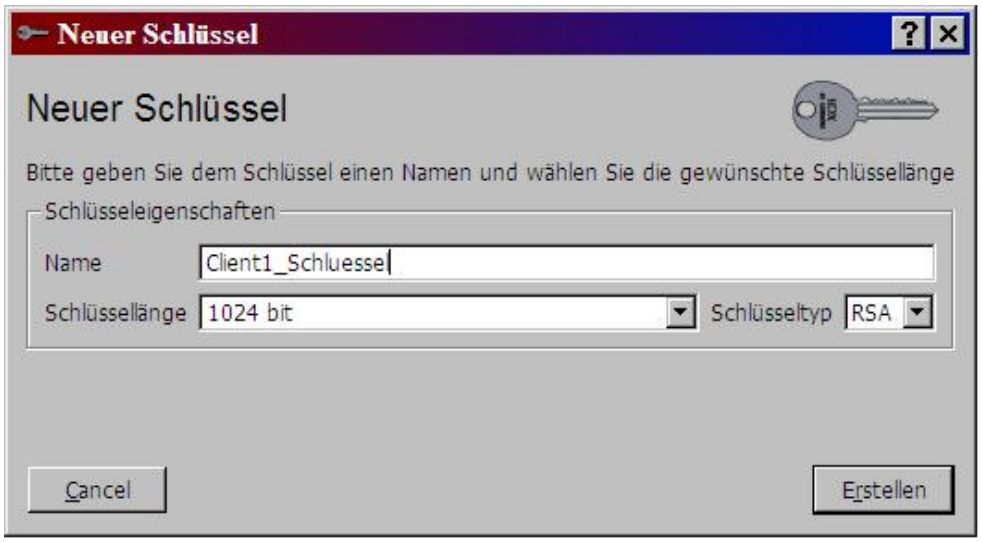


Abbildung 114

10.2.2.3 Clientzertifikat - Extensions

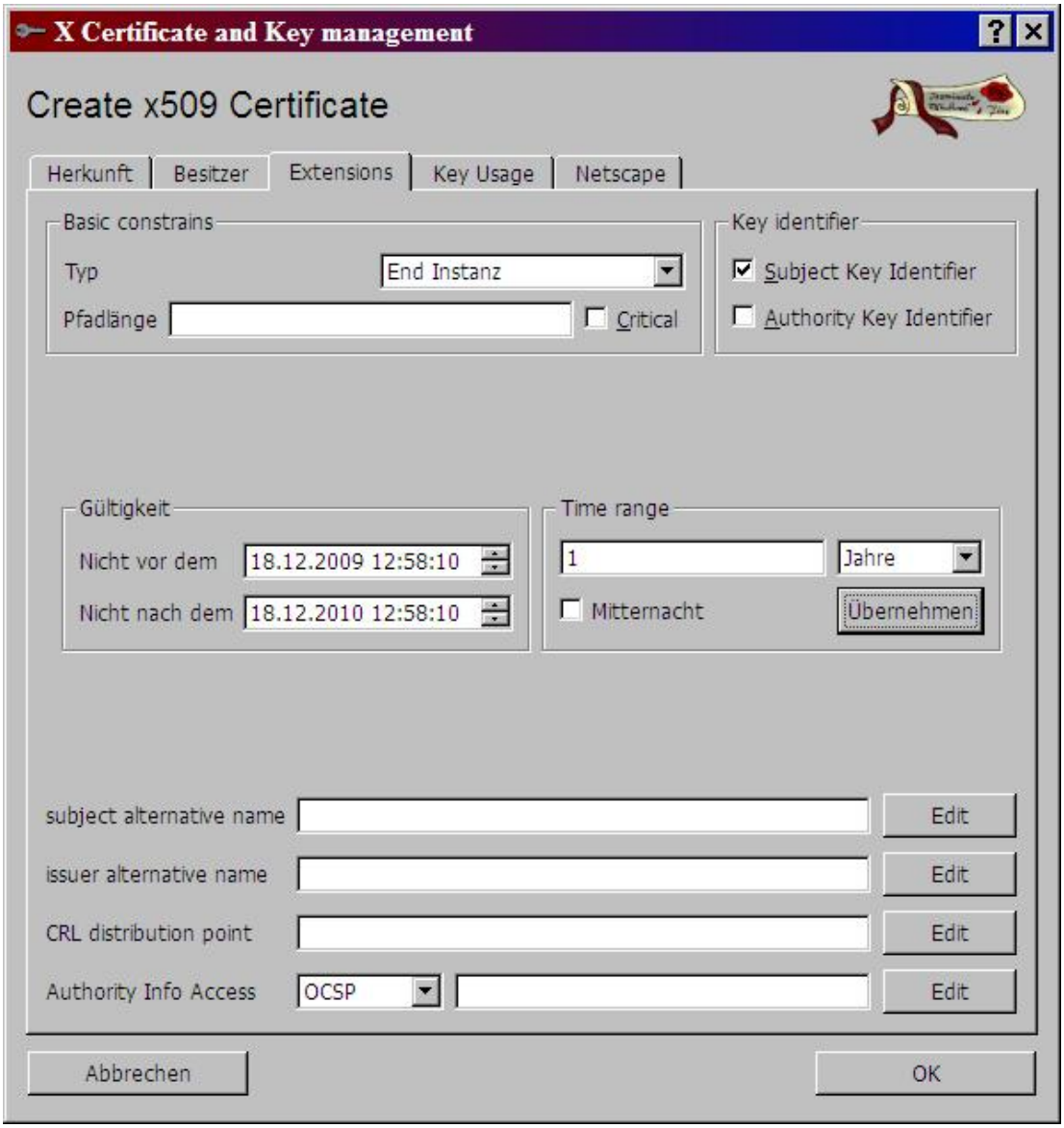


Abbildung 115

Da ihr Clientzertifikat keine anderen Zertifikate unterzeichnen muss, geben Sie bei Zertifikatstyp „Endinstanz“ ein.

Basic constrains
Typ = Endinstanz

Key identifier
Haken setzen bei Subject Key Identifier

Gültigkeit
Sie können das genaue Anfangs-/ und Enddatum in die ausgewiesenen Felder eingeben, oder den nebenstehenden Eintrag Time Range benutzen.

Time Range
Stellen Sie im Menü ganz rechts den Zahlenwert Tage, Monate oder Jahre ein. Welche Dauer einzelne Zertifikate haben sollten, sehen Sie in der unten angegebenen Aufstellung:

- Personenzertifikate sollten 1 Jahr Gültigkeit haben.
- Server (SSL) Zertifikate ebenfalls 1 Jahr Gültigkeit.
- Router Zertifikate sollten 1 (wenn es fremde Router sind) oder 10 Jahre (wenn es eigene Router sind) Gültigkeit haben.
- CA Zertifikate sollten auch eine lange Laufzeit haben (Bsp. >10 Jahre).

Bitte mit *„Übernehmen“* die Werte der **Time Range** übernehmen

Subject alternative name
Der alternative Name des Inhabers besteht aus einer Liste von alternativen Namen für den Inhaber des Zertifikates, diese Namen können, RFC822-Namen (E-Mail), DNS-Namen, X.400 Adressen, EDI-Namen, URIs oder IP-Adressen sein, im Grunde ist jedes strukturiertes Namenschema verwendbar. Bei PKIX muss diese Erweiterung kritisch sein, wenn das Subject-Feld im Zertifikat leer ist.

Issuer alternative name
Für alternative Namen des Austellers gilt dasselbe wie für den alternativen Namen des Inhabers.

CRL distribution point
Um einen öffentlichen Zugangspunkt für Rückhollisten benutzen zu können, muss die LDAP-/ bzw. HTTP-Adresse der Rückholliste Liste eingetragen werden. Es ist der Adresse immer ein **URI** (universal resource indicator) (z.B. URI:http://de.wikipedia.de) voran zu setzen. Das Feldtrennzeichen ist ein Doppelpunkt. Falls Sie lokale Rückhollisten besitzen, ist diese Option für Sie nicht von Bedeutung.

Authority Info Access
Diese PKIX Erweiterung definiert, wie weitere Information und Services der ausstellenden CA genutzt werden können. Darin können weitere Informationen über die CA (weitere Richtlinien, Stammzertifikate,...) oder Online Verifikation Services (z.B. OCSP) bereitgestellt werden. Vor allem wenn bei Zertifikatsanwendungen wie Secure Mail (S/MIME) nicht der ganze Zertifizierungspfad mitgeschickt wird, ist es für die prüfende Anwendung nett, wenn im Endzertifikat in dieser Erweiterung aufgeführt ist, wo das nächsthöhere CA-Zertifikat abzurufen ist.

10.2.2.4 Clientzertifikat - Key Usage

Wenn Sie ein Clientzertifikat als Endinstanz erstellen, benötigen Sie keine der hier einstellbaren Optionen. Sie können sofort zum nächsten Reiter wechseln.

10.2.2.5 Clientzertifikat - Netscape

Falls Sie zusätzliche Sicherheit wünschen, dann können Sie für ihre VPN-Teilnehmer, je nachdem welche Rolle die VPN-Teilnehmer übernehmen(Client oder Server), noch die Option SSL-Server oder SSL-Client auswählen.
Dies hat den Vorteil, dass bei OpenVPN abgefragt werden kann, ob ein VPN-Server zusätzlich mit SSL ausgestattet ist. Im mbNET kann diese Option auch aktiviert werden. Im Kapitel zu OpenVPN

wird näher auf diese Thematik und diese Einstellungsmöglichkeit eingegangen. Wenn Sie ihr Clientzertifkat mit beiden Punkten ausstatten, dann kann mit dem Zertifikat sowohl ein VPN-Client als auch ein VPN-Server ausgestattet werden

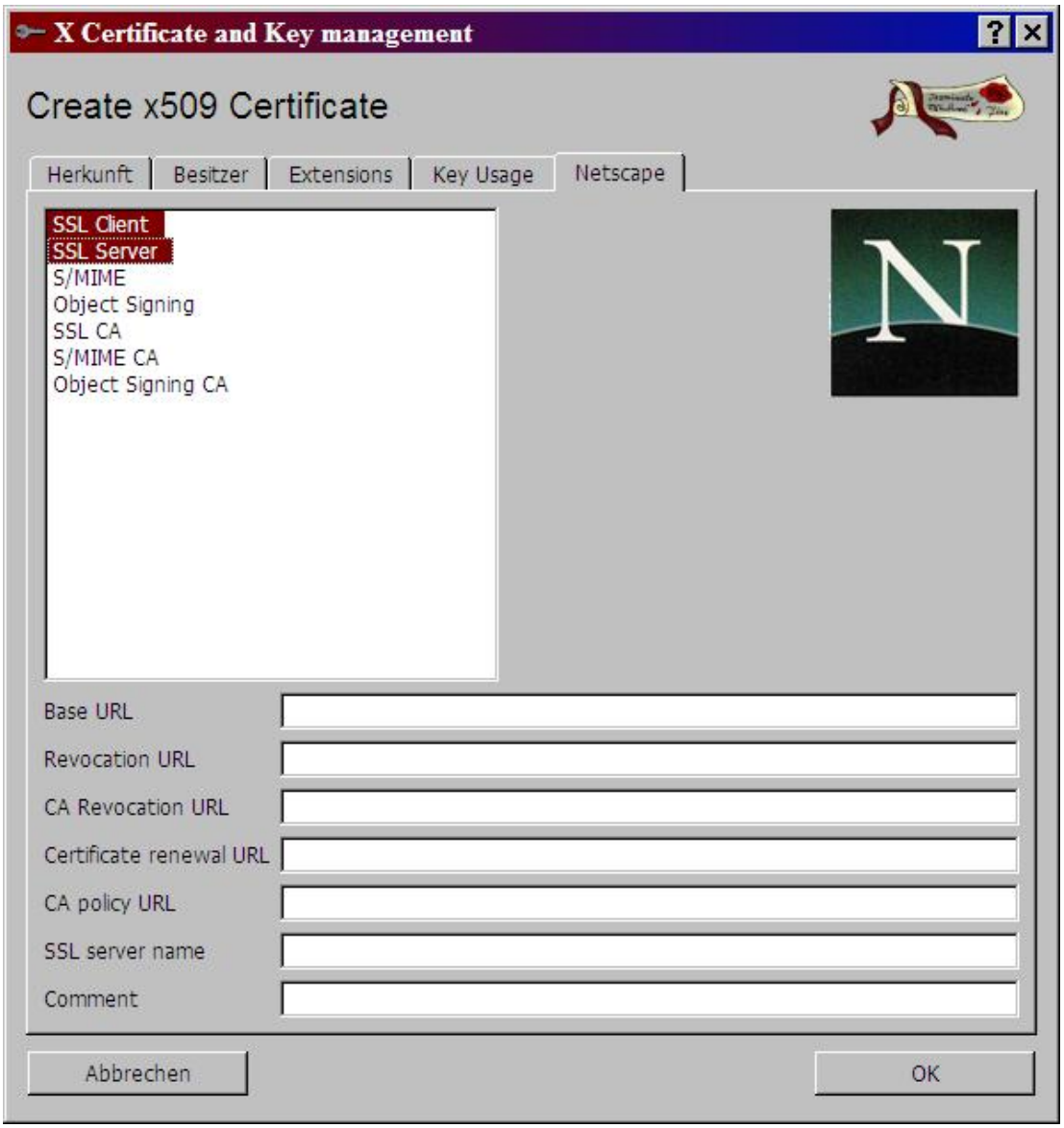


Abbildung 116

Im Reiter *„Netscape“* müssen für IP-Sec keine Einstellungen vorgenommen werden. Bei Verwendung von OpenVPN mit der aktivierten Option „Gegenstelle muss ein TLS-Server sein“ muss nur für das Server-Zertifikat die Option „SSL-Server“ ausgewählt werden. Beachten Sie dazu auch die Abbildung oben.

Nun müssen die erstellten Zertifikate im Reiter *„Zertifikate“* des ersten Dialogfeldes durch Markieren des jeweiligen Zertifikats und klicken auf *„Export“* verfügbar gemacht werden.

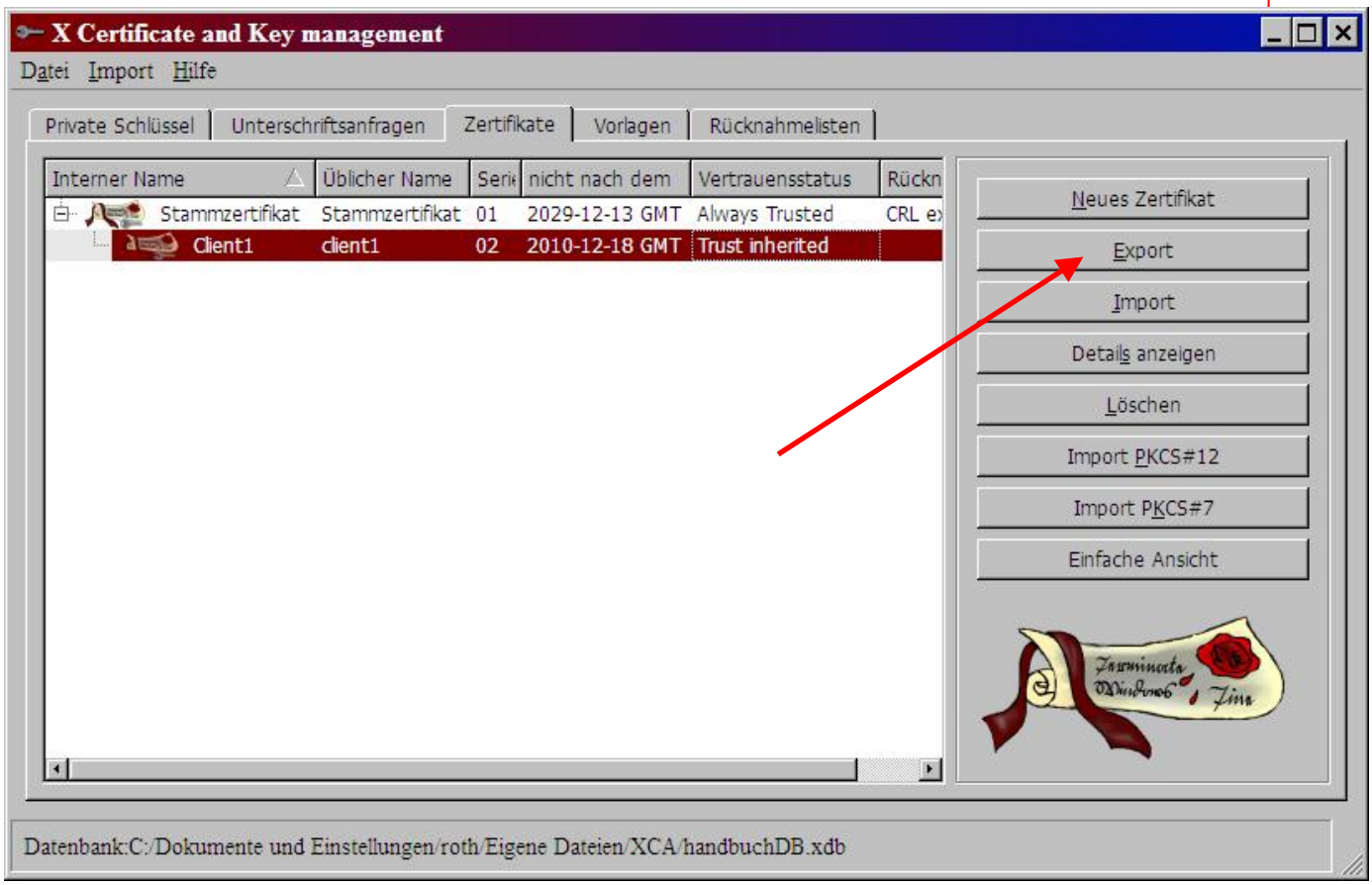


Abbildung 117

Im darauf folgenden Menü können Sie den Speicherort auf ihrem Computer für das Zertifikat festlegen und welches Format die Zertifikatsdatei haben soll.

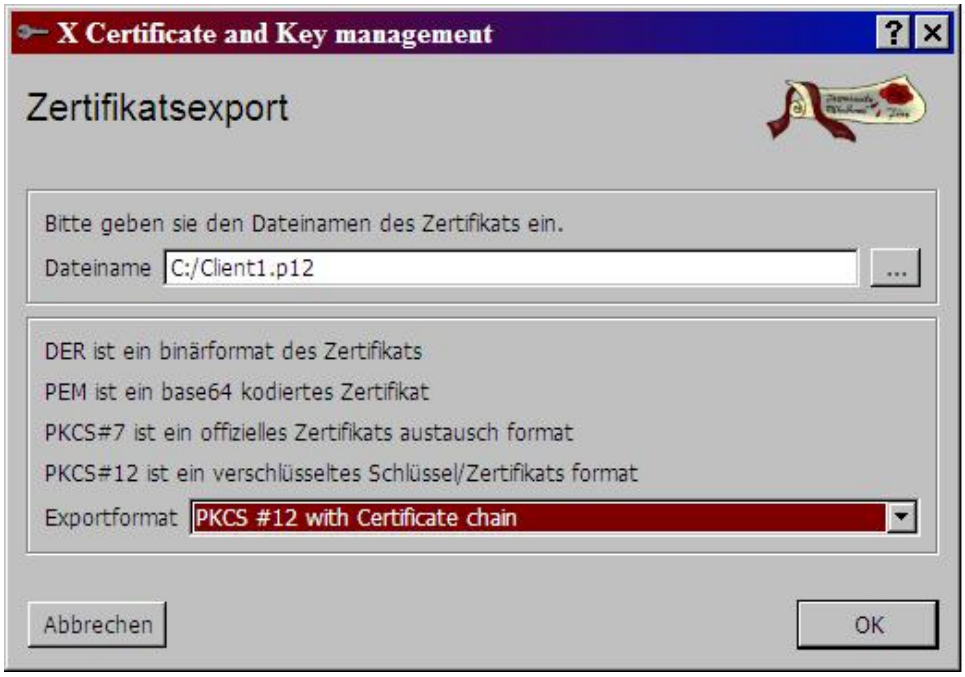


Abbildung 118

Da sich ihr Client mit dem Clientzertifikat authentifizieren soll, benötigt er zusätzlich zu diesem Clientzertifikat noch den passenden privaten Schlüssel. Exportieren Sie daher wie die Abbildung 118 zeigt, das Clientzertifikat im Format PKCS #12 with Certificate chain. Mit einem Klick auf OK wird das Clientzertifikat an den vorher angegebenen Ort gespeichert. Das Clientzertifikat hat dann die Endung .p12.

Das Stammzertifikat muss mit dem Format PEM (Dateiendung .crt) exportiert werden!

Diese Zertifikate können dann über die Weboberfläche auf den Router *mbNET* importiert werden (vgl. Kapitel **System - Zertifikate**)
Wie man einen Windowsclient mit diesen Zertifikaten ausstattet, wird in Kapitel **Zertifikate unter Windows XP importieren** erklärt.

10.3 Erstellen von CRL-Dateien (Widerrufslisten)

Wenn Sie einem Mitarbeiter die Berechtigung zur Verwendung des VPN-Tunnels entziehen wollen, dann lesen Sie bitte dieses Kapitel und erstellen sich eine Certificate Revocation List. Hierfür öffnen Sie erneut die Software XCA. Öffnen Sie die Datenbank, welche die Zertifikate Ihrer Mitarbeiter enthält. Um nun ein Zertifikat für ungültig zu erklären, klicken Sie es bitte einmal mit der rechten Maustaste an –es erscheint der folgende Dialog:

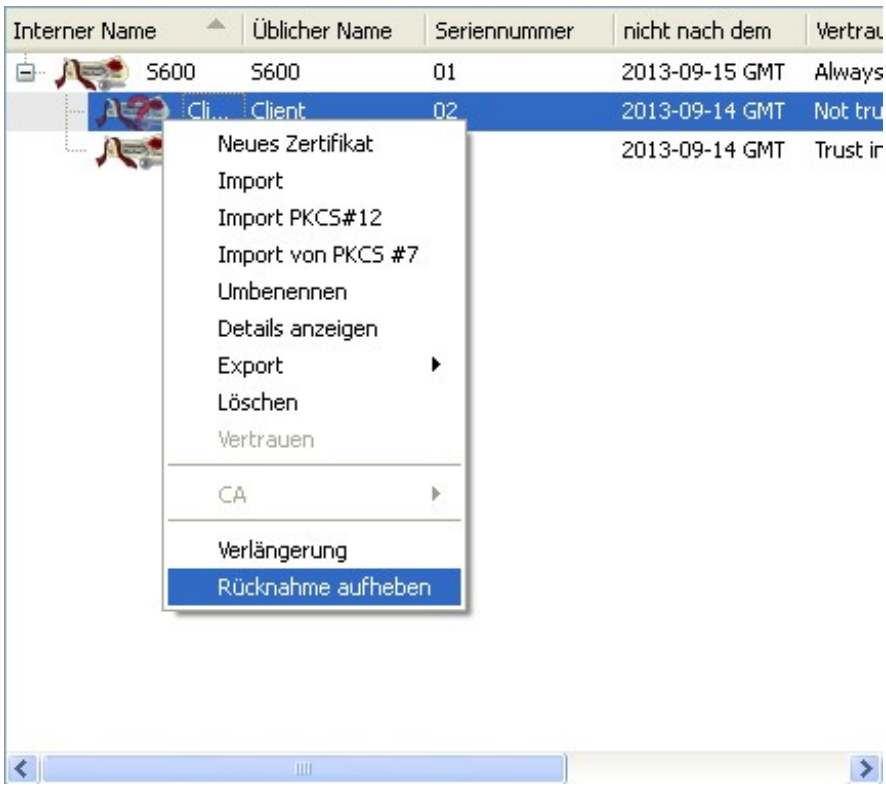


Abbildung 119

Klicken sie wie im Bild dargestellt auf *„Rücknahme“*. Der entsprechende Zertifikatseintrag wird mit einem roten Fragezeichen markiert und ist somit ungültig.

Im nächsten Schritt klicken Sie ebenfalls mit einem Rechstklick auf das zugehörige Stammzellenzertifikat. Es erscheint der folgende Dialog:

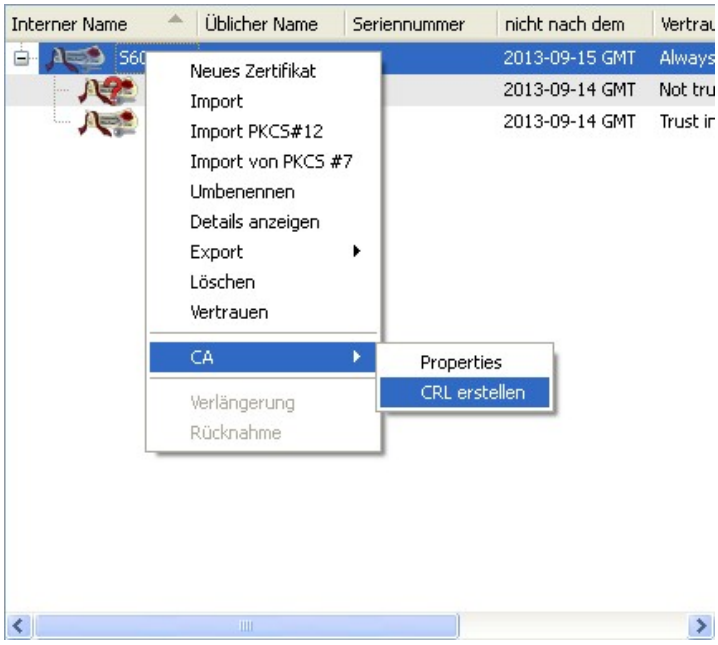


Abbildung 120

Hier können Sie nun wie im obigen Bild dargestellt über den Menüpunkt *„CA → CRL erstellen“* eine Widerrufsliste erstellen. Achten Sie bitte darauf auch hier beim „Hash Algorithmus“ MD5 auszuwählen. Bei Erweiterungen ist nichts durch einen Haken zu aktivieren. Die CRL muss nun exportiert und ins mbNET importiert werden. Zum Exportieren gehen Sie bitte wie folgt vor:

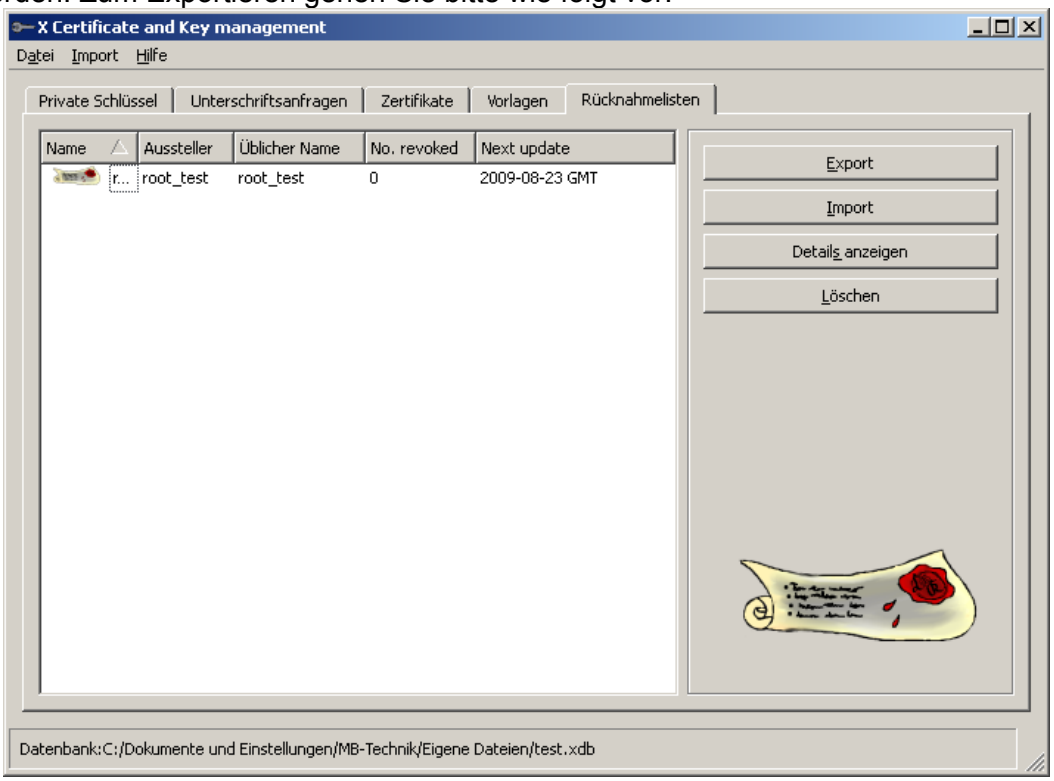


Abbildung 121

Unter der Registerkarte *„Rücknahmelisten“* sehen Sie nun Ihre soeben erstellte Widerrufsliste. Markieren Sie diese und klicken Sie dann auf *„Export“*. Als Exportformat wählen Sie bitte **.pem**. Bestätigen Sie mit OK, nachdem Sie sich für einen passenden Speicherort entschieden haben. Sie können nun diese Liste über den Menüpunkt **System → Zertifikate** auf der Weboberfläche des mbNET importieren (vgl. Kapitel CRL). Nachdem Sie die VPN-Verbindungen bzw. das mbNET neu gestartet haben wird die CRL aktiviert und ein Tunnelaufbau mit dem ungültigen Zertifikat ist nicht mehr möglich.

11. Zertifikate unter Windows XP importieren

Um bereits fertige Zertifikate zu importieren, müssen Sie eine so genannte Zertifikats-Management-Konsole erstellen. Geben Sie dazu unter *„Startmenü -> Ausführen „**MMC**“ ein*. Klicken Sie dann auf *„Datei - Snap-In hinzufügen/entfernen“* und wählen im darauf folgenden Dialog *„Hinzufügen“* aus. In der Liste der verfügbaren Snap-Ins kann dann **Zertifikate** ausgewählt werden.

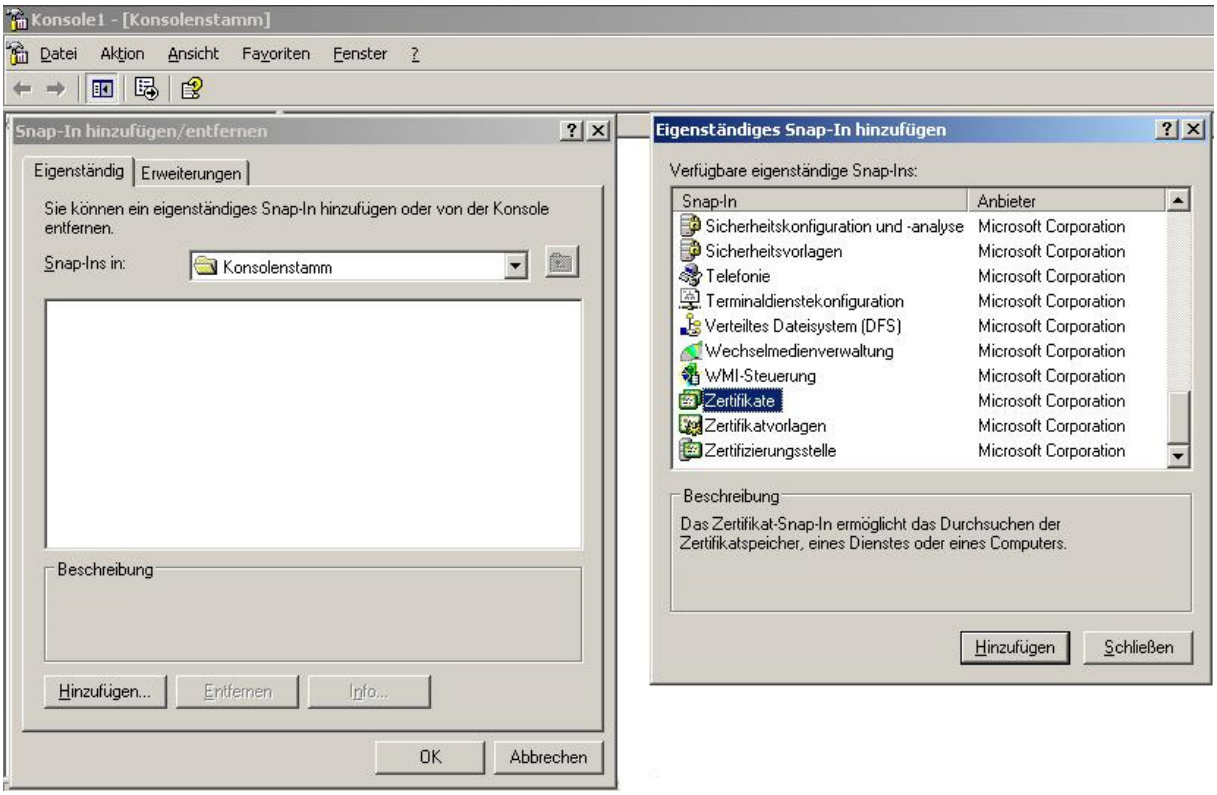


Abbildung 122

Wählen Sie im nächsten Schritt „*Computerkonto*“ aus:

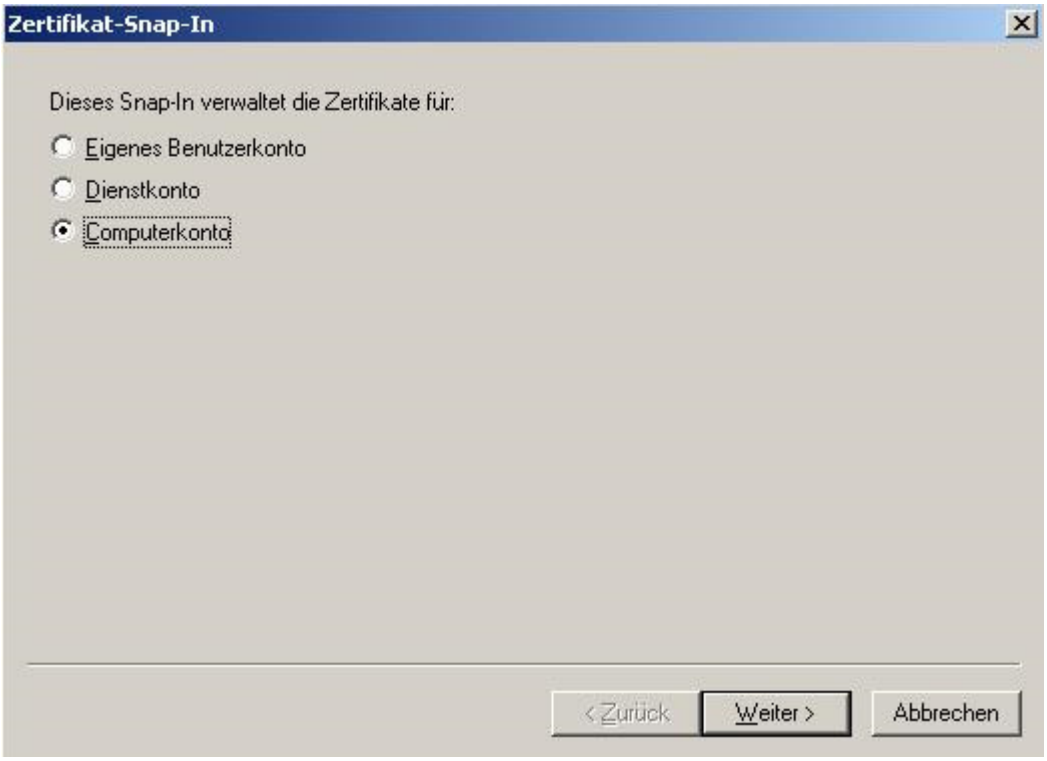


Abbildung 123

Im darauf folgenden Dialog muss unter der Rubrik *„Dieses Snap-In verwaltet“ „Lokalen Computer: (Computer, auf dem diese Konsole ausgeführt wird)“* ausgewählt werden.
Nachdem Sie die Zertifikatskonsole nun so erstellt haben, können Sie ein **Zertifikat importieren**. Zunächst öffnen Sie mit einem Rechtsklick auf *„Eigene Zertifikate -> Zertifikate“* den unten abgebildeten Dialog und importieren das Zertifikat, mit dem sich der Client ausweisen soll. Achten Sie hierbei darauf die **„.p12“-Datei** auszuwählen. Geben Sie das Kennwort für die p12-Datei ein und klicken dann auf weiter. Wählen Sie in der nächsten Dialogbox *„Zertifikatsspeicher automatisch auswählen (auf dem Zertifikatstyp basierend)“*. Mit einem Klick auf *„Fertigstellen“* werden die nötigen Zertifikate importiert.

Es sind keine weiteren Zertifikate zu importieren. Das CA-Zertifikat wird automatisch mit importiert. Es ist außerdem nicht zwingend von Nöten die erstellte Konsole abzuspeichern.

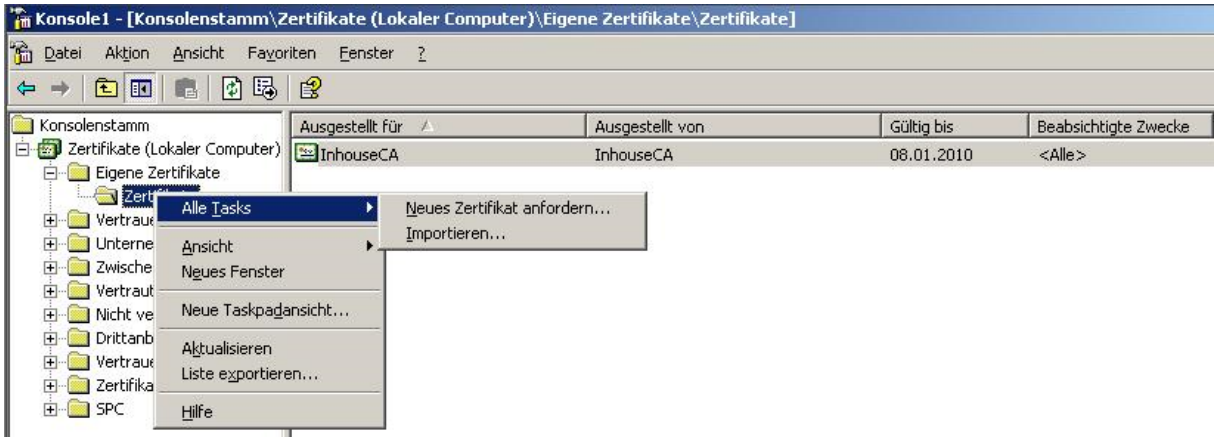


Abbildung 124

Durch einen Doppelklick auf das gewünschte Zertifikat gelangen Sie in dessen Eigenschaften. Sie können im Reiter *„Allgemein“* u. a. überprüfen, von welcher CA das Zertifikat ausgestellt wurde, wie

lang das Zertifikat noch gültig ist und ob Sie einen privaten Schlüssel für dieses Zertifikat besitzen. Dieser Punkt ist sehr wichtig für die Verwendung von Zertifikaten in Webserververöffentlichungen.

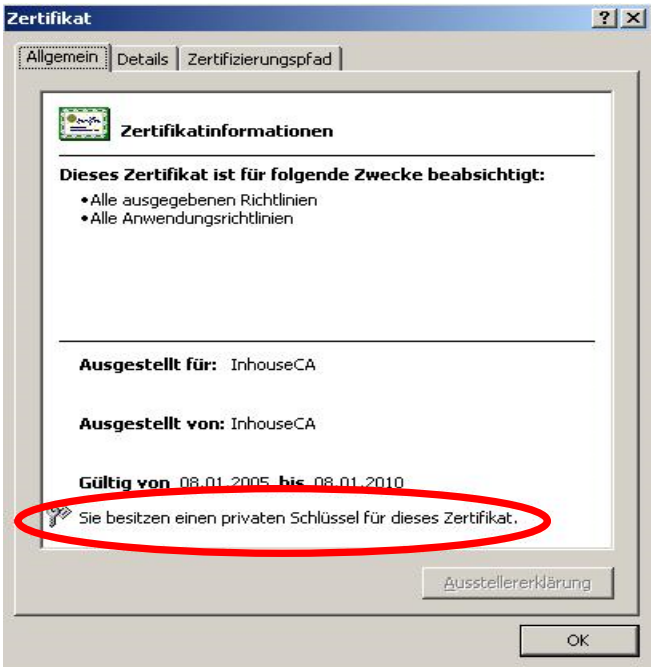


Abbildung 125

Im Reiter *„Details“* erhalten Sie weitere Informationen über das ausgestellte Zertifikat.

Abbildung 126

12. Systemeinstellungen

Im **Kapitel** Systemeinstellungen sind die wichtigsten Systemeinstellungen bereits beschrieben. Daneben gibt es noch weitere Systemeinstellungen, die im Folgenden näher beschrieben werden.

12.1 System – WEB

Bei der Verwendung von HTTPS (= Hypertext Transfer Protocol Secure, engl. = sicher; zuerkennen im Browserfenster an https ://...) wird die Verbindung zwischen Webbrowser und -Webserver verschlüsselt. Je nach Schlüssellänge meistens 40 oder 128 Bit.

Abbildung 127

Bezeichnung	Beschreibung
HTTP Port	Der Standardport für HTTP-Anfragen ist 80 TCP. Sollten Sie diesen Port jedoch für ihre OpenVPN-Verbindung benötigen, oder er schon anderweitig verwendet wird.
HTTPS aktivieren	Durch Anklicken der Checkbox kann das sichere Hypertext Transfer Protocol aktiviert werden.
HTTPS Port	Für den Zugriff sind vom entfernten Rechner die IP-Adresse des Routers und der Port einzugeben. Hier: Port 443

12.2 System – Benutzer

12.2.1 Allgemeines

Über das Benutzermanagement können Sie:

- ❑ Benutzern Zugriff auf die Administration der Weboberfläche, Modem-Einwahl oder VPN-Einwahl erlauben.
- ❑ vorhandene Benutzer editieren, löschen oder neue Benutzer anlegen.

12.2.2 Benutzer editieren

Zum Editieren eines Benutzers gehen Sie bitte folgendermaßen vor:

- ❑ Wählen Sie **System** und dann **Benutzer**.
- ❑ Betätigen Sie den **Knopf** um einen Benutzer dessen Rechte Sie ändern möchten auszuwählen.
  Der Benutzer wird zusammen mit den Zugangseinstellungen in der ersten Zeile angezeigt.

Abbildung 128

- ❑ Wechseln Sie in die entsprechenden Eingabefelder und führen Sie die Änderungen durch.
- ❑ Speichern Sie ihre Änderung mit einem Druck auf Speichern
  (Diskette Abbildung 129)

Abbildung 129

- ❑ Sie können jetzt noch Ihre letzten Änderungen über die Schaltfläche **Änderungen löschen** zurücksetzen.

Abbildung 130

- ❑ Über die Schaltfläche Änderungen übernehmen werden die Änderungen auf den Industrierouter übertragen.

Abbildung 131

12.2.3 Benutzer anlegen

Zum Anlegen eines Benutzers gehen Sie bitte folgendermaßen vor:

- Wählen Sie in der linken Navigationsleiste **System** und dann **Benutzer**.

Abbildung 132

- Tragen Sie in die Eingabefelder der ersten Zeile den **Benutzernamen**, das **Passwort** und den **vollständigen Namen** des Benutzers ein.

Bitte beachten Sie!
Es müssen immer alle drei Eingabefelder ausgefüllt werden, ansonsten wird beim Speichern eine Fehlermeldung ausgegeben.

- ❑ Legen Sie über die drei folgenden Auswahlboxen fest, welche Rechte der neue Benutzer erhalten soll. Wählen Sie aus, ob der Benutzer.
  - Einstellungen an der Weboberfläche durchführen darf (Administration).
  - eine Verbindung zum Modem des Industrierouters herstellen darf (Modem-Einwahl)
  - eine Verbindung auf den Industrierouter über VPN herstellen darf (VPN-Einwahl)
- ❑ Zutreffendes ist durch Anklicken der entsprechenden **Auswahlbox** mit einem Häkchen zu versehen.
- ❑ Klicken Sie zum temporären Speichern nun auf die Schaltfläche „Änderungen speichern“.

Abbildung 133

Abbildung 134

Abbildung 135

Zum Übertragen der Einstellungen auf den Industrierouter betätigen Sie die Schaltfläche **Änderungen übernehmen**

12.2.4 Benutzer löschen

Zum Löschen eines Benutzers gehen Sie bitte folgendermaßen vor:

- ❑ Wählen Sie in der linken Navigationsleiste **System** und dann **Benutzer**
- ❑ Wählen Sie die Zeile aus, in der der Benutzer mit Passwort usw. aufgeführt ist und klicken Sie auf das Symbol **Löschen**

Abbildung 136

Zum dauerhaften Speichern der Einstellungen auf den Industrierouter betätigen Sie die Schaltfläche **Änderungen übernehmen**

Abbildung 137

Sie können sich nun nicht mehr mit diesem Benutzer an der Weboberfläche, der Modem-/ oder VPN-Einwahl anmelden bzw. authentifizieren

12.3 System - Zertifikate

Hauptbestandteil bei VPN-Verbindungen mit IPSec sind die Vertrauensstellungen zwischen zwei oder mehreren Kommunikationspartnern. Die Authentifizierung wird bei der IPSec-Konfiguration unter Kapitel **Authentisierung** eingestellt.
Für eine sichere Kommunikation ist die Prüfung der Authentizität erforderlich. Mit Hilfe von Zertifikaten wird sichergestellt, dass auch die ***richtigen*** Partner miteinander kommunizieren. Mit einem Zertifikat weist sich der Zertifikatsinhaber aus. Das Zertifikat kann von einer übergeordneten Stelle (sog. Certificate Authority kurz CA) oder vom Zertifikatsinhaber selbst ausgestellt werden. Der Zertifikatsinhaber wird dabei mit ***Subject***, der Zertifikatsaussteller mit ***Issuer*** bezeichnet.
Nachfolgend die Bildschirmmaske mit den Registerkarten der entsprechenden Zertifikate und der Möglichkeit neue Zertifikate zu importieren.

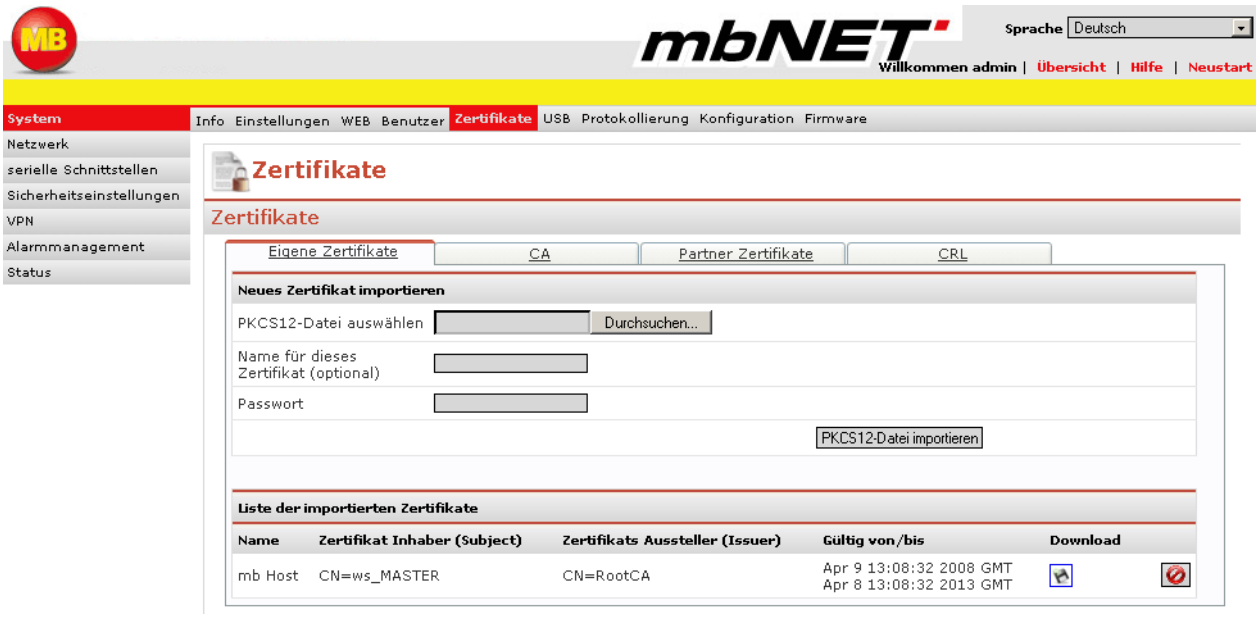


Abbildung 138

12.3.1 Eigene Zertifikate

Eigene Zertifikate werden vom Zertifikatsinhaber selbst ausgestellt. Damit der Router das eigene Zertifikat bei einer Gegenstelle verwenden kann, um es dort vorzuzeigen, ist die entsprechende PKCS12-Datei(Zertifikat inklusive privatem Schlüssel) auszuwählen, um diese dann zu importieren. Es können dabei eine oder mehrere PKCS12-Dateien importiert werden. Zum eigenen Zertifikat gehört auch immer ein Schlüssel. Daher muss hier eine PKCS12-Datei importiert werden. Diese besteht nämlich aus einer .crt-Datei und einer .pem Schlüsseldatei.

Bitte beachten Sie, dass XCA den Schlüssel und das Zertifikat zu einer Datei zusammenfasst, deren Dateiendung „ .p12 “ ist. Hiermit ist jedoch die PKCS12-Datei gemeint.

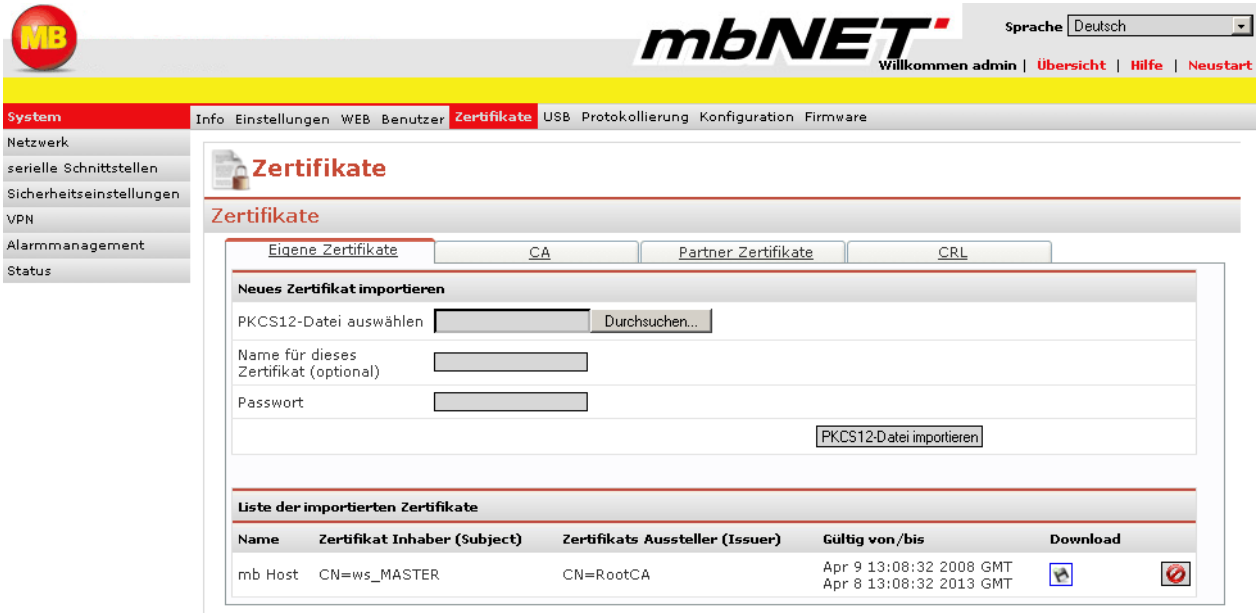


Abbildung 139

Bezeichnung	Beschreibung			
Neue Zertifikate importieren	**PKCS12-Datei auswählen:** Auswahl der Zertifikatsdatei (PKCS12-Datei). **Durchsuchen:** Angabe des Speicherortes der Zertifikatsdatei. **Name für dieses Zertifikat (optional):** Optionale Eingabe des Namens für die Zertifikatsdatei. **Passwort**: Eingabe des Zertifikatspasswortes. Beim Erstellen des Zertifikats muss ein Passwort vergeben worden sein, ansonsten wird das Importieren nicht möglich! **PKCS12-Datei importieren:** Falls die obigen Eingaben korrekt eingeben sind, kann die Zertifikatsdatei durch einen Druck auf den Knopf importiert werden.			
Liste der importierten Zertifikate	Hier werden bereits die importierten Zertifikate aufgelistet. Weitere Zertifikatsdateien können über **PKCS12-Datei importieren** aufgenommen werden.			
Name	Name für das Zertifikat: hier: mb Host			
Zertifikat Inhaber (Subject)	Merkmale des Zertifikatinhabers – Hier im Beispiel:			
	C		OU	
	ST		CN	Ws_MASTER
	L		emailAdress	
	O			

Eigene Zertifikate (Fortsetzung)

Bezeichnung	Beschreibung	
Zertifikats Aussteller	Beschreibung siehe vorhergehende Seite **Zertifikat Inhaber (Subject)**.	
Gültig von / bis	Anzeige des Zeitraumes während dem das Zertifikat Gültigkeit besitzt.	
Download		Nach Betätigen dieser Schaltfläche erscheint ein weiterer Bereich. Zum Download ist mit der rechten Maustaste auf den Link zu klicken und die Option **Ziel speichern unter ....** auszuwählen.
		Nach Betätigen dieser Schaltfläche kann die Liste der importierten Zertifikate zurückgesetzt bzw. gelöscht werden.

12.3.2 CA

Durch ein Stammzertifikat wird überprüft, ob das Zertifikat von der Gegenstelle auch von dem Stammzertifikat signiert ist. Ein solches Stammzertifikat muss dann importiert werden, wenn unter den VPN-Einstellungen als Authentisierungsmethode „durch ein Zertifikat von der selben CA“ gewählt wird. Als Entscheidungskriterium ob das Zertifikat des sich Einwählenden gültig ist, wird dann der Eintrag im Stammzertifikat hergenommen. Das CA-Zertifikat enthält nämlich Informationen darüber, ob das Zertifikat der Gegenstelle gültig ist oder nicht.
Das CA-Zertifikat steht in Dateiform (CRT-Datei) zur Verfügung und ist auf den Router zu importieren.

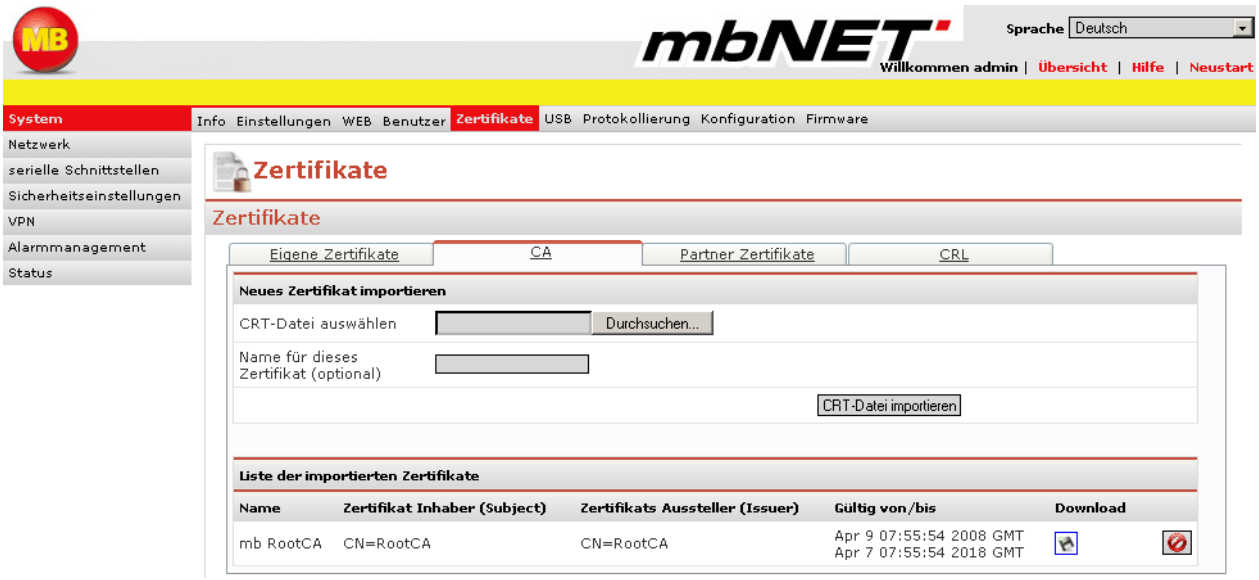


Abbildung 140

Bezeichnung	Beschreibung
Neue Zertifikate importieren	**CRT-Datei auswählen:** Manuelle Eingabe des Speicherortes oder Durchsuchen des entsprechenden Laufwerkes nach der Zertifikatsdatei. (Dateinamen-Erweiterung: .crt) **Name für dieses Zertifikat (optional):** Optionale Eingabe des Namens für die Zertifikatdatei. Wird kein Name angegeben, dann wird automatisch der Generelle Name (Common Name) verwendet **CRT-Datei importieren:** Falls die obigen Eingaben korrekt eingeben sind, kann die Zertifikatsdatei hiermit importiert werden.
Liste der importierten Zertifikate	Hier werden bereits die importierten Zertifikate aufgelistet. Weitere Zertifikatsdateien können über **CRT-Datei importieren** aufgenommen werden. Weitere Infos zu ***Namen***, ***Zertifikat Inhaber (Subject)***, ***Zertifikats Aussteller (Issuer)***, ***Gültig von / bis*** und ***Download*** entnehmen Sie bitte dem Kapitel Eigene Zertifikate

12.3.3 Partner Zertifikate

Partner Zertifikate sind Zertifikate der Gegenstelle. Sie werden nur benötigt, wenn man in den VPN-Einstellungen „Authentisierung durch Partnerzertifikat“ gewählt hat. Dann nämlich gilt als Entscheidungskriterium für die Gültigkeit eines Zertifikats, dass eine Kopie dieses Zertifikats lokal vorliegt.
Das Zertifikat der Gegenstelle ist über die entsprechende crt-Datei auszuwählen und dann zu importieren. Es können auch mehrere crt-Dateien importiert werden.

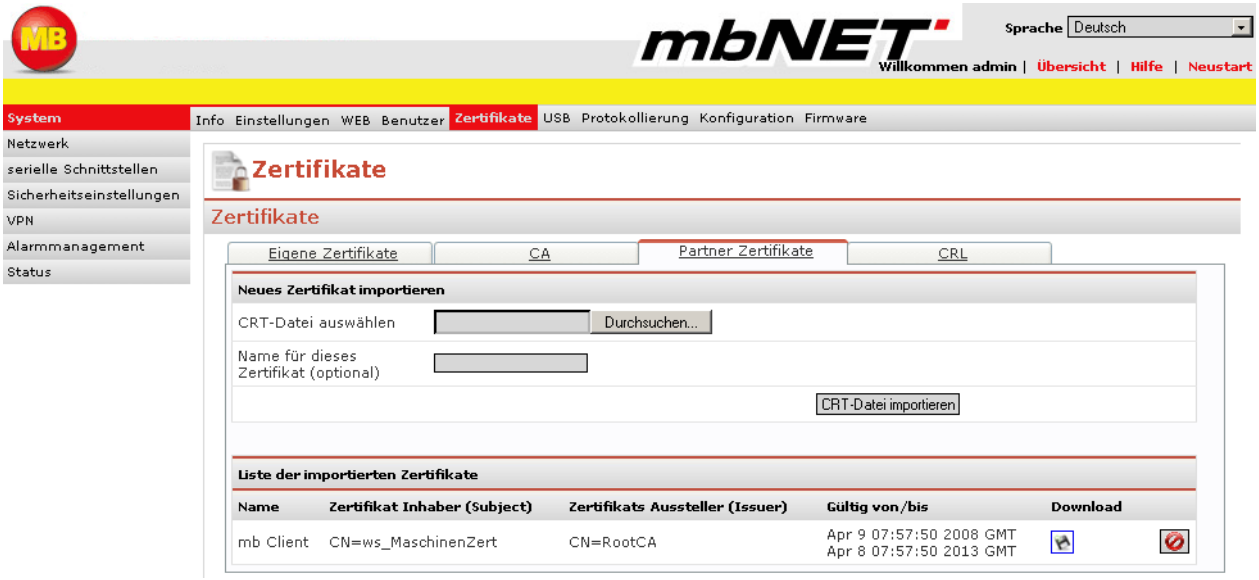


Abbildung 141

Bezeichnung	Beschreibung
Neue Zertifikate importieren	**CRT-Datei auswählen:** Manuelle Eingabe des Speicherortes oder Durchsuchen des entsprechenden Laufwerkes nach der Zertifikatsdatei. (Dateinamen-Erweiterung: .crt) **Name für dieses Zertifikat (optional):** Optionale Eingabe des Namens für die Zertifikatdatei. **CRT-Datei importieren:** Falls die obigen Eingaben korrekt eingeben sind, kann die Zertifikatsdatei importiert werden.
Liste der importierten Zertifikate	Hier werden bereits die importierten Zertifikate aufgelistet. Weiter Zertifikatsdateien können über **CRT-Datei importieren** aufgenommen werden. Weitere Infos zu ***Namen***, ***Zertifikat Inhaber (Subject)***, ***Zertifikats Aussteller (Issuer)***, ***Gültig von / bis*** und ***Download*** entnehmen Sie bitte dem Kapitel **Eigene Zertifikate**

12.3.4 CRL

Über die Rückhol-/ und Sperrliste (Certificate Revocation Liste kurz CRL) wird überprüft, ob die Zertifikate von sich einwählenden Rechnern gültig sind oder nicht.
Die CRL enthält die Seriennummern von Zertifikaten die gesperrt werden sollen. Wenn man also Personen, die Berechtigung zur Einwahl auf den Router oder die dahinterliegende SPS entziehen will, so muss lediglich eine CRL erstellt werden. Dies ist mit XCA leicht zu realisieren.

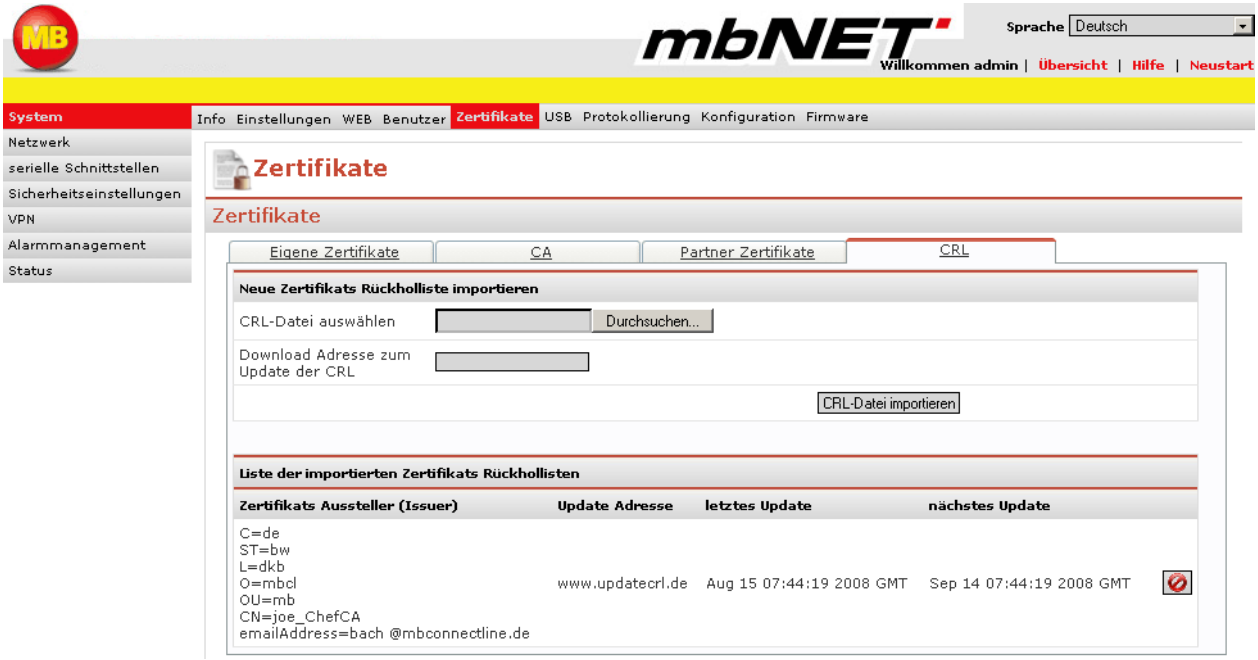


Abbildung 142

Bezeichnung	Beschreibung
Neue Zertifikate importieren	**PEM-Datei auswählen:** Manuelle Eingabe des Speicherortes oder Durchsuchen des entsprechenden Laufwerkes nach der Sperrdatei. (Dateinamen-Erweiterung: .pem) **Download Adresse zum Update der CRL:** Die PEM-Datei kann regelmäßig bei Angabe der Download Adresse erneuert werden. **PEM-Datei importieren:** Falls die obigen Eingaben korrekt eingeben sind, kann die Sperrdatei importiert werden.
Liste der importierten Zertifikate	Hier werden bereits die importierten Zertifikate aufgelistet. Weiter Zertifikatsdateien können über **PEM-Datei importieren** aufgenommen werden. Weitere Infos zu ***Namen***, ***Zertifikat Inhaber (Subject)***, ***Zertifikats Aussteller (Issuer)***, ***Gültig von / bis*** und ***Download*** entnehmen Sie bitte dem Kapitel **Eigene Zertifikate**
Zertifikats Aussteller (Issuer)	Siehe Kapitel **Eigene Zertifikate**
Update Adresse	Anzeige der Update Adresse für die Sperrdatei.
Letztes Updates	Anzeige wann das letzte Update der Sperrdatei stattfand.
Nächstes Update	Anzeige wann das nächste Update der Sperrdatei durchgeführt werden soll.

12.4 System - USB

Am USB-Anschluss des Industrierouters können Sie ein USB-Gerät (Speicherstick oder USB-Festplatte) anschließen und diese für die Benutzer des Netzwerkes als zusätzliches Laufwerk freigeben.
Zur Einrichtung des USB-Anschlusses drücken Sie in der linken Navigationsleiste auf **System** und in der oberen Navigationsleiste auf **USB**. Es wird die nachfolgende Bildschirmmaske angezeigt.

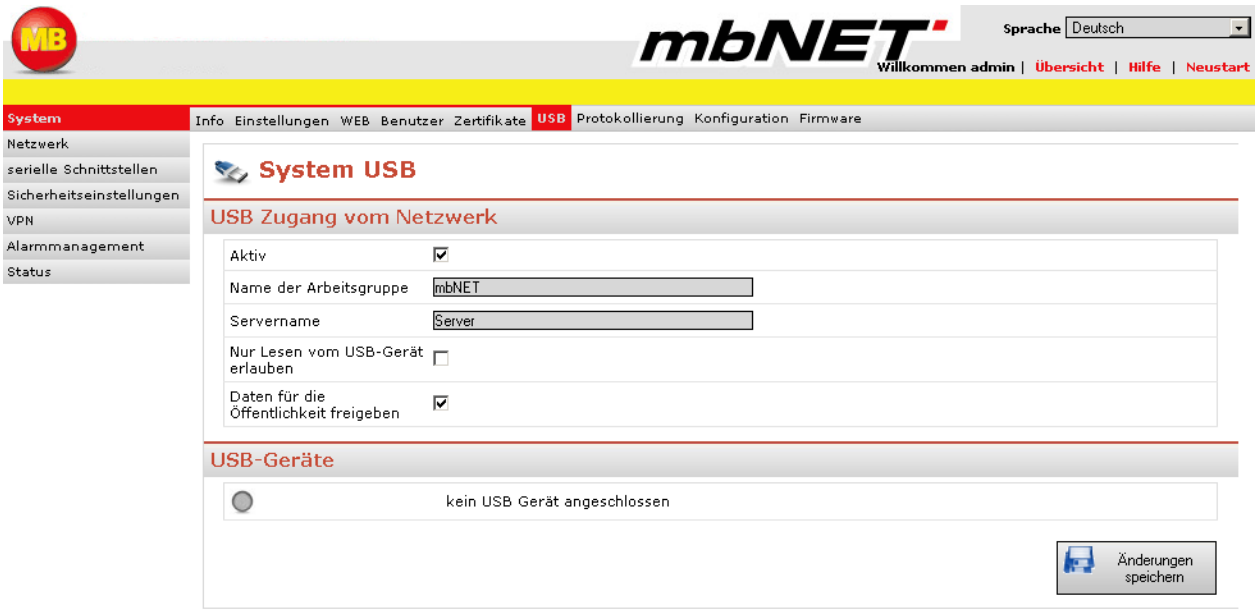


Abbildung 143

Bezeichnung	Beschreibung
Aktiv	Wählen Sie hiermit aus, ob ein angeschlossener USB-Speicher vom Industrierouter eingebunden werden soll.
Name der Arbeitsgruppe	Tragen Sie hier den Namen der Arbeitsgruppe ein, über die die Benutzer auf den Speicher zugreifen können.
Servername	Tragen Sie einen Namen ein, unter dem der USB-Speicher in der oben angegebenen Arbeitsgruppe erscheint.
Nur Lesen von USB-Gerät erlauben	Wählen Sie aus, ob die Benutzer auf den USB-Speicher nur lesend zugreifen dürfen, oder auch auf den USB-Speicher Daten abspeichern können.
Daten für Öffentlichkeit freigeben	Legen Sie fest, ob Benutzern im Netzwerk, die nicht in der Benutzerverwaltung des Industrierouters eingetragen sind, der Zugriff auf den USB-Speicher erlaubt ist.
USB-Gerät	Im unteren Bereich der Bildschirmmaske wird angezeigt, ob ein USB-Gerät angeschlossen ist. Falls ein USB-Gerät angeschlossen ist, wird dies symbolisch durch einen grün ausgefüllten Kreis dargestellt.

Bitte beachten Sie, dass die Speichermedien den Dateisystemtyp FAT/FAT32 besitzen müssen. Mit anderen Dateisystem wie z.B. NTFS kann es zu Problemen kommen.

12.5 System - Protokollierung

Mit Hilfe eines Protokollierungsservers kann die Systemprotokollierung des *mbNET* auf einen anderen Rechner ausgelagert werden.

Abbildung 144

Bezeichnung	Beschreibung
Externen Protokollierungsserver aktivieren	Zur Auswahl eines Protokollierungsservers ist die Checkbox durch Anklicken mit einem Häkchen zu versehen. Hiermit kann die Systemprotokollierung des Industrierouters *mbNET* auf einen anderen Rechner ausgelagert werden.
IP-Adresse des Protokollierungsserver	IP-Adresse des Protokollierungsservers. Hier: 192.168.0.65
Port des externen Protokollierungsserver	Portangabe des Protokollierungsservers. Hier: Port 514 Wir empfehlen diesen Port nicht zu ändern, es sei denn Sie haben eine Anwendung die auf einen komplett anderen Port reagiert.

12.6 System - Konfiguration

Die Systemkonfiguration kann hiermit sowohl gespeichert, als auch wiederhergestellt werden. Über einen angeschlossen USB-Speicher z.B. kann die Konfiguration vor dem Durchführen größerer Änderungen gespeichert und notfalls wieder auf den Industrierouter wiederhergestellt werden.

Abbildung 145

Bezeichnung	Beschreibung
Name der Konfiguration	Vergabe eines sinnvollen Namens für die Konfiguration. Hier: *mbNET*
Sichern	Konfiguration sichern. Nach Anklicken der Schaltfläche wird man aufgefordert den Ort z.B. Laufwerksbuchstabe des USB-Speichermediums anzugeben.
Sicherung mit Zertifikaten und Schlüsseldateien	Hiermit wird eine Konfiguration angelegt um ein mbNET zu kopieren. Bitte beachten Sie, dass diese Konfigurationsdatei nur für ein Gerät verwendet wird.
Auf USB-Gerät speichern	Falls ein USB Speichermedium am mbNET angeschlossen ist, so kann die Konfiguration auch dort gespeichert werden.
Überschreibe vorhandene Konfiguration	Ist die Möglichkeit nicht aktiviert und ist eine Konfigurationsdatei schon an demselben Speicherort vorhanden, dann wird die neue Konfiguration nicht gespeichert. Entweder Sie benennen eine der Dateien um, oder benutzen einen anderen Speicherort für die neue Konfigurationsdatei.
Gespeicherte Konfigurationsdatei (.mbn):	Zum Wiederherstellen einer Konfiguration muss die entsprechend gespeicherte Datei in der die Konfiguration des Industrierouters enthalten ist, wieder hergestellt, d.h. wieder zurück auf den Router übertragen werden. Zum Wiederherstellen ist zuerst die Schaltfläche **Durchsuchen** zu betätigen, Danach Speicherort bzw. Verzeichnis in dem sich die Datei befindet, auswählen Daraufhin die Taste **Wiederherstellen** betätigen.
Konfiguration von USB-Gerät laden	Ist eine Konfigurationsdatei auf dem Speichermedium des mbNET angeschlossen, dann wird wie oben im Beispiel die Datei(en) angezeigt. Sie können dann eine der Dateien anwählen und auf **Wiederherstellen** drücken. Im Anschluss daran werden Sie gefragt welche Bereiche der Konfiguration Sie wiederherstellen möchten. Aktivieren Sie die gewünschten Bereiche und bestätigen den Vorgang. Zuletzt werden Sie aufgefordert, das Gerät neuzustarten.

12.7 System - Firmware

Die Aktualisierung der Firmware auf dem Industrierouter kann auf zwei Arten wie nachfolgend dargestellt, durchgeführt werden.

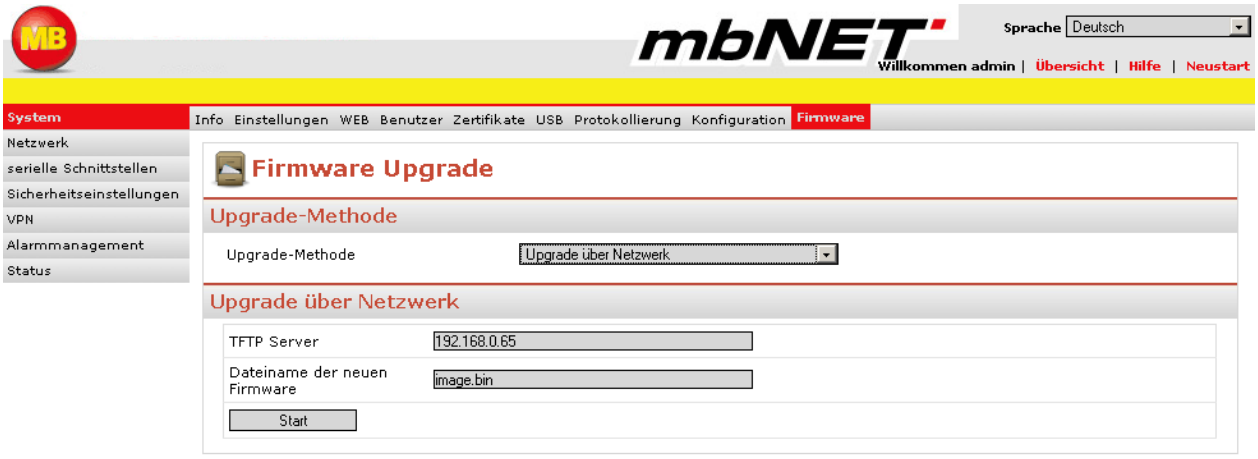
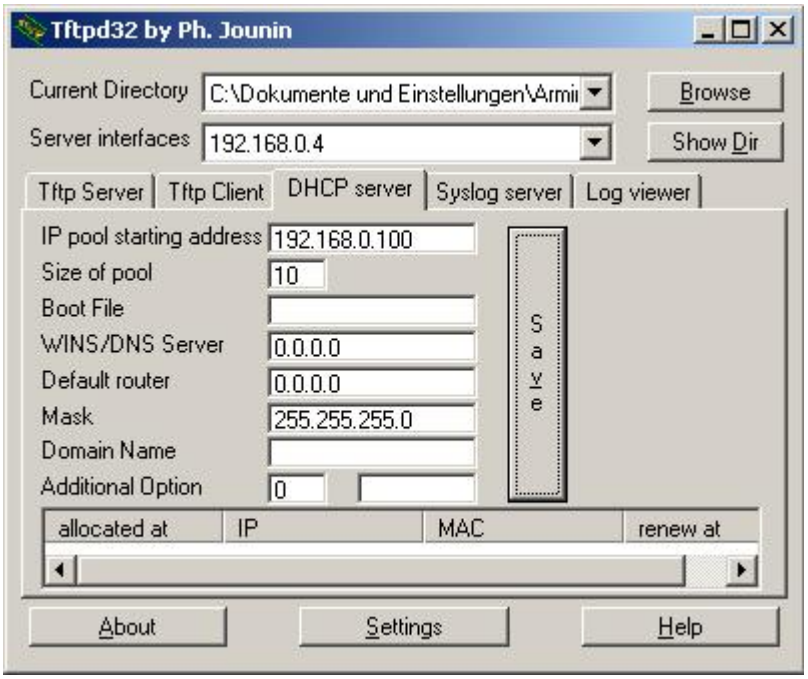


Abbildung 146

Bezeichnung	Beschreibung
Upgrade-Methode	Nach Anklicken des Auswahlfeldes stehen folgende zwei Möglichkeiten der Firmwareaktualisierung zur Verfügung: **Upgrade über USB:** Hierbei muss ein USB-Speichergerät am Industrierouter angeschlossen sein, damit die Datei auf den Industrierouter übertragen werden kann. Hier ist der Firmwarename (Name lautet „image.bin“) eingetragen. Zum Übertragen der Firmware ist die Schaltfläche **Start** zu betätigen. Danach müssen Sie das Gerät neu starten. **Upgrade über Netzwerk:** Hierbei muss die IP-Adresse eines TFTP-Servers und der Firmwarename eingetragen werden. Hier: image.bin Bevor das Upgrade beginnen kann muss das Tool „tftpd32“ gestartet werden. Dieses kann auf der Seite http://tftpd32.jounin.net/ kostenlos heruntergeladen werden. Wenn das Tool gestartet wurde, muss unter dem Register „DHCP server“ folgendes eingestellt werden: IP pool starting address: *IP-Adresse des Routers der hochgerüstet werden soll* Size of pool: *10* Mask: *Subnetzmaske des Netzwerks*  **Abbildung 147** Mit Klicken auf den Knopf **save** werden die Einstellungen gespeichert. Im Auswahlfeld „Current Directory“ muss der Ordner ausgewählt werden, in dem die Firmware-Datei für das Firmware-Upgrade abgelegt ist. Das Tool darf während des Upgrades nicht geschlossen werden. Nun muss auf der Web-Oberfläche die Adresse des Computer auf dem Tftpd32 gestartet ist in das Feld TFTP-Server eingetragen werden. Drücken Sie nun auf die Schaltfläche **Start**. Danach müssen Sie das Gerät neu starten. **UNTERBRECHEN SIE NIEMALS DAS MBNET WÄHREND EINER ERNEUERUNG DER FIRMWARE!!!!!!! Das Gerät kann sonst nicht mehr starten**

13. Netzwerk

13.1 Netzwerk - LAN

Über die LAN-Konfiguration lässt sich die IP-Adresse (LAN-Adresse) und die Subnetzmaske des Routers konfigurieren. Über diese IP-Adresse ist der Router im LAN-Netzwerk erreichbar.

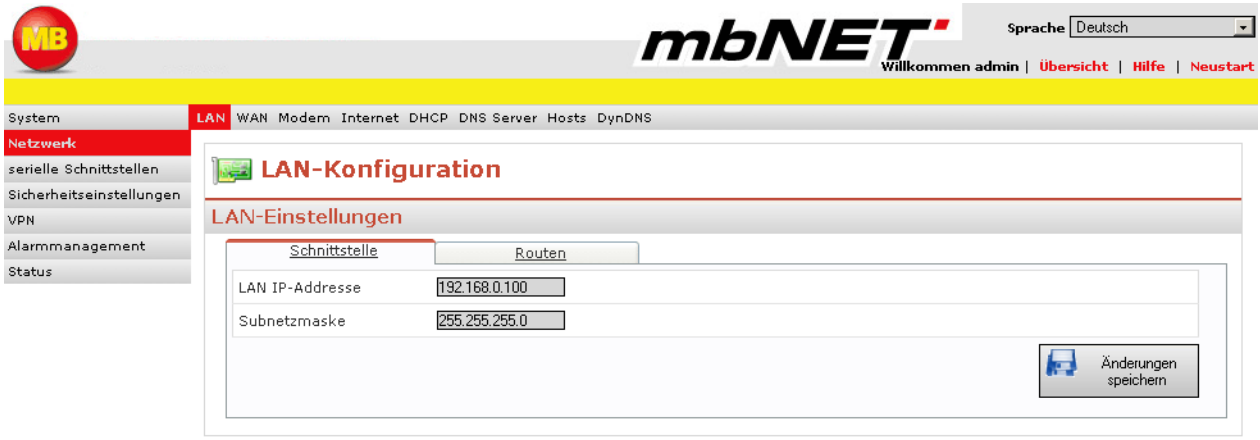


Abbildung 148

Bezeichnung	Beschreibung
Schnittstelle	Zur Einstellung der LAN-Schnittstelle ist die Registerkarte anzuklicken.
LAN-IP-Adresse	Eintrag der entsprechenden IP-Adresse des Routers.
Subnetzmaske	Eintrag der Subnetzmaske des entsprechenden Netzwerks, in dem der Router integriert werden soll.
Routen	Zur Einstellung bestimmter Routen ist die Registerkarte Routen anzuklicken. Hier können sowohl Netzrouten in CIDR-Form (x.x.x.0/24) als auch Hostrouten angegeben werden.

13.2 Netzwerk - WAN

Die WAN-Schnittstelle des Industrierouters kann ein lokales Netzwerk mit einem weiteren Netzwerk oder dem öffentlichen Netzwerk, wie das Internet, verbinden. Die WAN-Schnittstelle ist deshalb hierzu anwendungsabhängig zu konfigurieren.

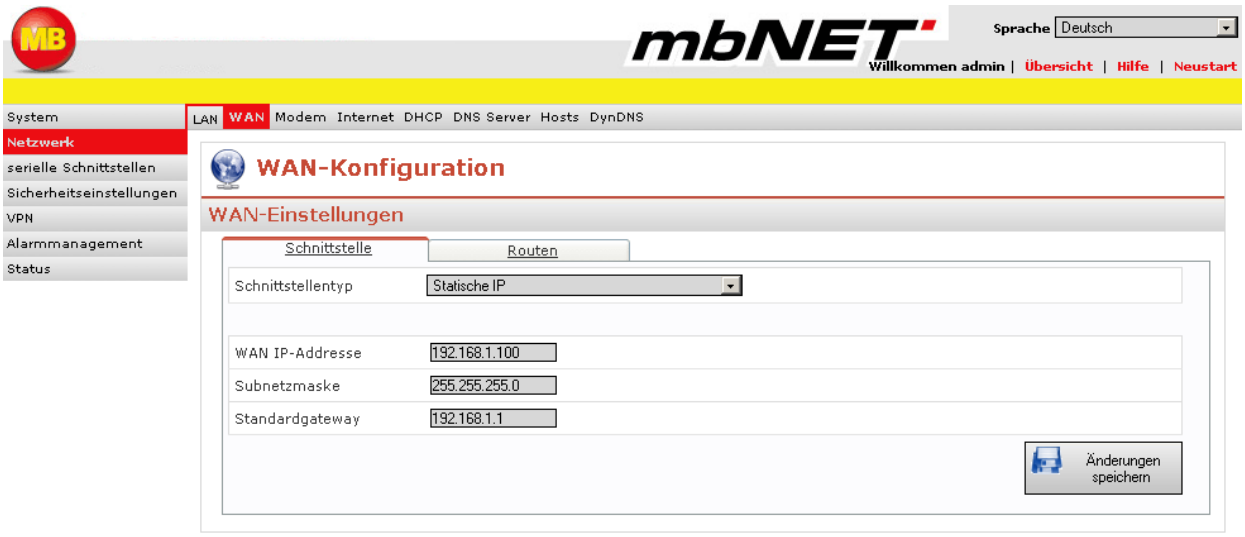


Abbildung 149

Bezeichnung	Beschreibung
Schnittstel-lentyp	Folgende Schnittstellentypen können ausgewählt werden: **DSL:** Wählen Sie diesen Option, wenn Ihr Router direkt mit einem DSL-Modem verbunden ist, das die Verbindung ins Internet herstellt. **DHCP:** Wählen Sie diese Einstellung, wenn ein DHCP-Server im Netzwerk vorhanden ist und somit der Industrierouter automatisch eine IP-Adresse zugewiesen bekommt. **Wenden Sie sich diesbezüglich auch an Ihren Netzwerkadministrator** **Statische IP:** Wählen Sie diese Einstellung, wenn ein bereits vorhandener Router die Verbindung ins Internet herstellt und dieser nicht als DHCP-Server, bzw. keine Adressenvergabe durch einen Server vorgegeben ist. Diese Einstellung ist auch zu wählen, wenn Sie von Ihrem ISP eine statische Adresse erhalten haben z.B. bei einer Standleitung. Weiterhin muss beachtet werden, dass bei dieser Art der Verbindung ein DNS-Server eingetragen werden muss (siehe Kapitel **Netzwerk - DNS-Server**). **WAN-IP-Adresse:** IP-Adresse des Routers am WAN-Anschluss. **Subnetzmaske:** Eingabe der Subnetzmaske. **Standardgateway:** Geben Sie hier das entsprechende Gateway ein, das Sie mit dem Internet verbindet, also die IP-Adresse des bestehenden Routers.

Netzwerk - WAN (Fortsetzung)

Bezeichnung	Beschreibung
Verbindungs-modus	**Bei Auswahl des Schnittstellentyps DSL ist zusätzlich eine der nachfolgende Optionen auszuwählen:** **PPPoE:** Wählen Sie diese Option aus, wenn Ihr Internetserviceprovider eine PPPoE-Verbindung (Point-To-Point Protocol over Ethernet) erfordert. Diese Option wird bei vielen Modems eingestellt. Die externe IP-Adresse unter der der Router von einer entfernten Gegenstelle aus erreichbar ist, wird vom Internetprovider festgelegt. Bitte entnehmen Sie die notwendigen Informationen den Unterlagen Ihres Providers. **PPP Benutzer:** Geben Sie hier Ihren Benutzernamen ei. Entnehmen Sie den Benutzernamen den Zugangsdaten Ihres Providers. **PPP Passwort:** Geben Sie hier Ihr Passwort ein. Entnehmen Sie das Passwort den Zugangsdaten Ihres Providers. **PPTP:** Wählen Sie diese Option aus, wenn Ihr Internetserviceprovider eine PPTP-Verbindung (Point-To-Point Tunneling Protocol) erfordert. In Österreich wird z.B. PPTP zur DSL-Anbindung verwendet. **PPP Benutzer:** Entnehmen Sie den Benutzernamen den Zugangsdaten Ihres Internetdiensanbieters. **PPP Passwort:** Entnehmen Sie das Passwort den Zugangsdaten Ihres Internetdienstanbieters. **WAN-IP-Adresse:** Geben Sie hier die IP-Adresse des Routers *mbNET* am WAN-Anschluss ein. Es handelt sich hierbei um eine Adresse unter der der Router von Geräten erreichbar ist, die sich auf der Seite des **WAN** Anschlusses befinden. Falls Ihnen die IP-Adresse Ihres Internet Providers nicht automatisch zugewiesen wird, tragen Sie hier die IP-Adresse unter der der Router vom PPTP-Server aus erreichbar ist, manuell ein. Bitte entnehmen Sie die notwendigen Informationen den Unterlagen Ihres Providers **Subnetzmaske:** Tragen Sie hier die Netzmaske des am LAN Anschluss angeschlossenem Netzwerk ein. **PPTP Server IP-Adresse:** Tragen sie hier die IP-Adresse des Servers Ihres Internet Providers ein.
Routen	Optional können hier Routen zu anderen Netzwerken definiert werden. Sind am lokal angeschlossen Netz weitere untergeordnete Netze angeschlossen, können Sie hier zusätzliche Routen definieren. Hier können sowohl Netzrouten in CIDR-Form (x.x.x.0/24) oder Routen zu einzelnen Netzteilnehmer angegeben werden.

13.3 Netzwerk - Modem

13.3.1 Netzwerk-Modem-Eingehend

Das im Industrierouter integrierte Modem ist für Wähl-/ und Internetverbindungen (Analog, ISDN, GSM) vorgesehen, wenn kein entsprechender DSL- oder Netzwerkanschluss vorhanden ist.

HINWEIS:
Wird das Modem für eine ausgehende Internetverbindung genutzt, so kann keine eingehende Verbindung erfolgen.

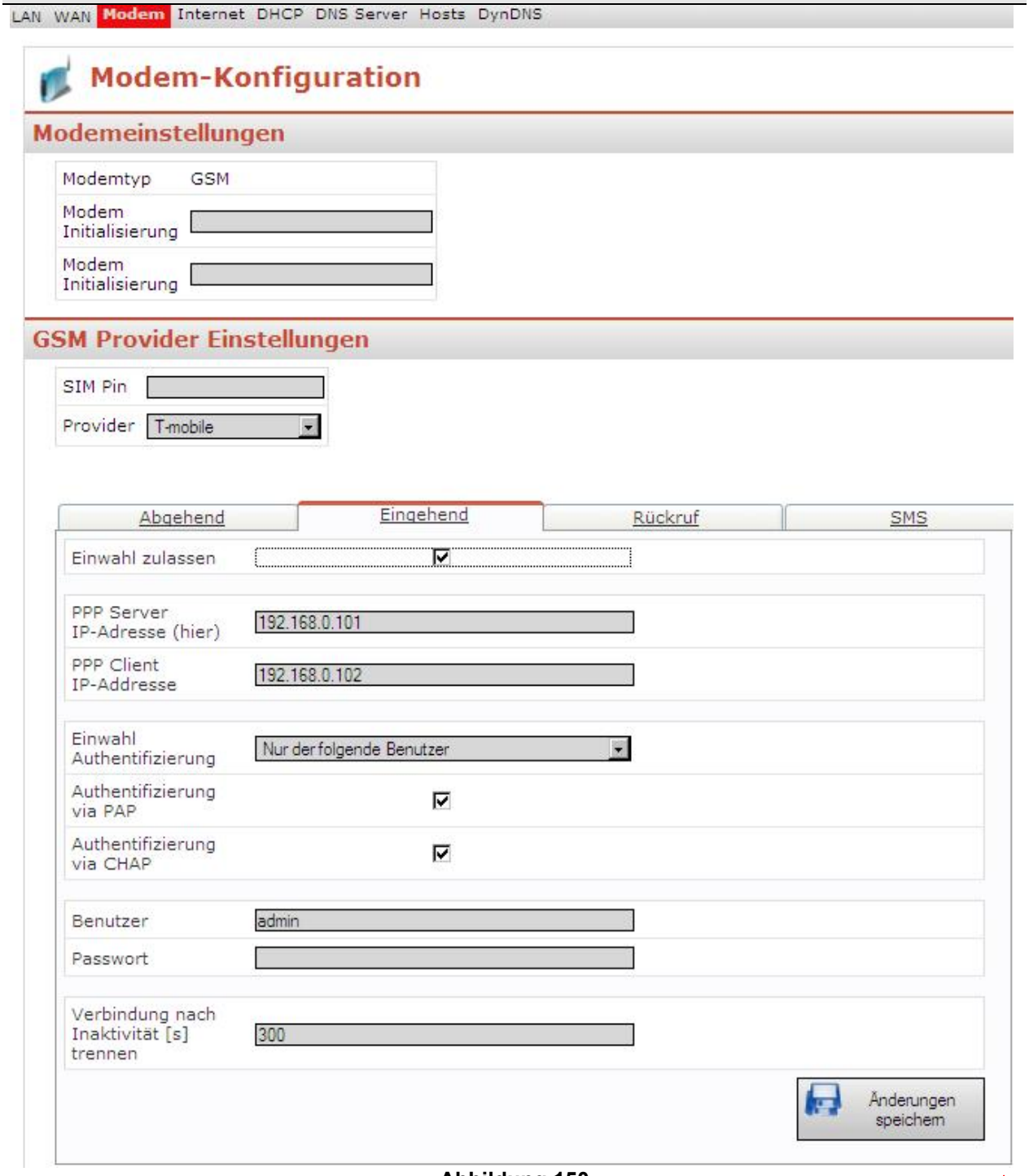


Abbildung 150

Bezeichnung	Beschreibung
Modem Initialisierung	**ANALOG:** Wenn Sie ein analoges Gerät verwenden, dann müssen Sie hier den Befehl **+GCI=Ländercode** (Ländercode siehe Kapitel **Ländercodes für analoge Geräte**) und in die zweite Zeile den Befehl **X3** (nicht auf Freizeichen warten) eingeben. **ISDN:** Wenn Sie ein ISDN-Gerät verwenden, dann müssen Sie mit dem Befehl **AT#Z=n** (n= MSN-Nummer) ihre MSN-Nummer eingeben. Geben Sie für „n“ einen „*“ ein, dann wird jeder Anruf angenommen. **GSM:** Wenn sie ein GSM-Gerät verwenden, dann müssen sie nur den voreingestellten Befehl X3 beibehalten. Der Befehl **+GCI=Ländercode** darf nicht verwendet werden.
SIM-PIN (nur bei GSM)	Hier kann, falls notwendig, der Pin für die SIM-Karte eingegeben werden.
Provider (nur bei GSM)	Hier kann der Mobilfunkanbieter ausgewählt werden. Falls der Anbieter nicht dabei ist, können Sie den APN auch von Hand eingeben. Informationen zum APN bekommen sie von unserer Internetseite unter http://www.mbconnectline.de/gsm/grps/gsm/grps.html oder Ihrem Anbieter.

Bezeichnung	Beschreibung
Eingehend	Um analoge Einwahlverbindungen oder per ISDN auf dem Router zu ermöglichen, ist diese Option zu aktivieren.
Einwahl zulassen	Die Funktion müssen Sie durch Anklicken mit einem Häkchen versehen, um den Zugriff von einem Client-Computer auf den Router freizugeben.
PPP Server IP-Adresse (hier)	Hier ist die IP-Adresse des Routers einzutragen Es ist möglich den gleichen Netzbereich wie den des lokalen Netzes zu verwenden. Achten Sie aber bitte darauf, dass die vergebenen Adressen nicht nochmals benutzt werden. Ansonsten kann es zu Adressenkonflikten kommen.
PPP Client IP-Adresse	Hier ist die IP-Adresse einzutragen, die der Router dem Client (anrufende Gegenstelle) zuteilt, sobald eine PPP-Verbindung zustande gekommen ist. Der Router und die Gegenstelle bilden somit nach dem Verbindungsaufbau ein eigenes Netzwerk.
Einwahl Authentifizierung	Stellen Sie hier ein, ob für die Einwahl auf den Router eine Abfrage von Benutzername und Passwort (sog. Authentifizierung) erforderlich ist. Folgende Auswahlen sind möglich: ❑ Nur der folgende Benutzer: nur der in den nachfolgenden Eingabefeldern eingetragene Benutzer ist berechtigt, eine Einwahl auf den Router durchzuführen. ❑ Jeder Benutzer mit Einwahlrechten: jeder Benutzer der im Benutzermanagement mit „Modem“-Rechten eingetragen wurde ist berechtigt eine Verbindung aufzubauen.
Authentifizierung via PAP / CHAP	Übernehmen Sie die werksseitige Voreinstellung. PAP/CHAP sind Authentifizierungsarten. Gleichen Sie diese Einstellung mit der des einwählenden Partners ab. Eine Deaktivierung von PAP/CHAP, hat zur Folge, dass diese Authentifizierung nicht akzeptiert wird und ihre gesendeten Daten auch für Andere lesbar sind.
Benutzername & Passwort	Geben Sie hier den Benutzernamen und das zugehörige Passwort für die PPP-Einwahl ein. Diese Felder sind nur vorhanden wenn die Option „Nur der folgende Benutzer“ bei Einwahl Authentifizierung gewählt wurde.
Verbindung nach Inaktivität [s] trennen	Hier ist die Zeit anzugeben, nach der eine bestehende Verbindung abgebaut wird, wenn während dieser Zeit keine Datenpakete übertragen werden. Falls nichts eingegeben wird, oder bei Eintrag „0“, wird die Verbindung nicht abgebaut.

13.3.2 Netzwerk-Modem-Ausgehend

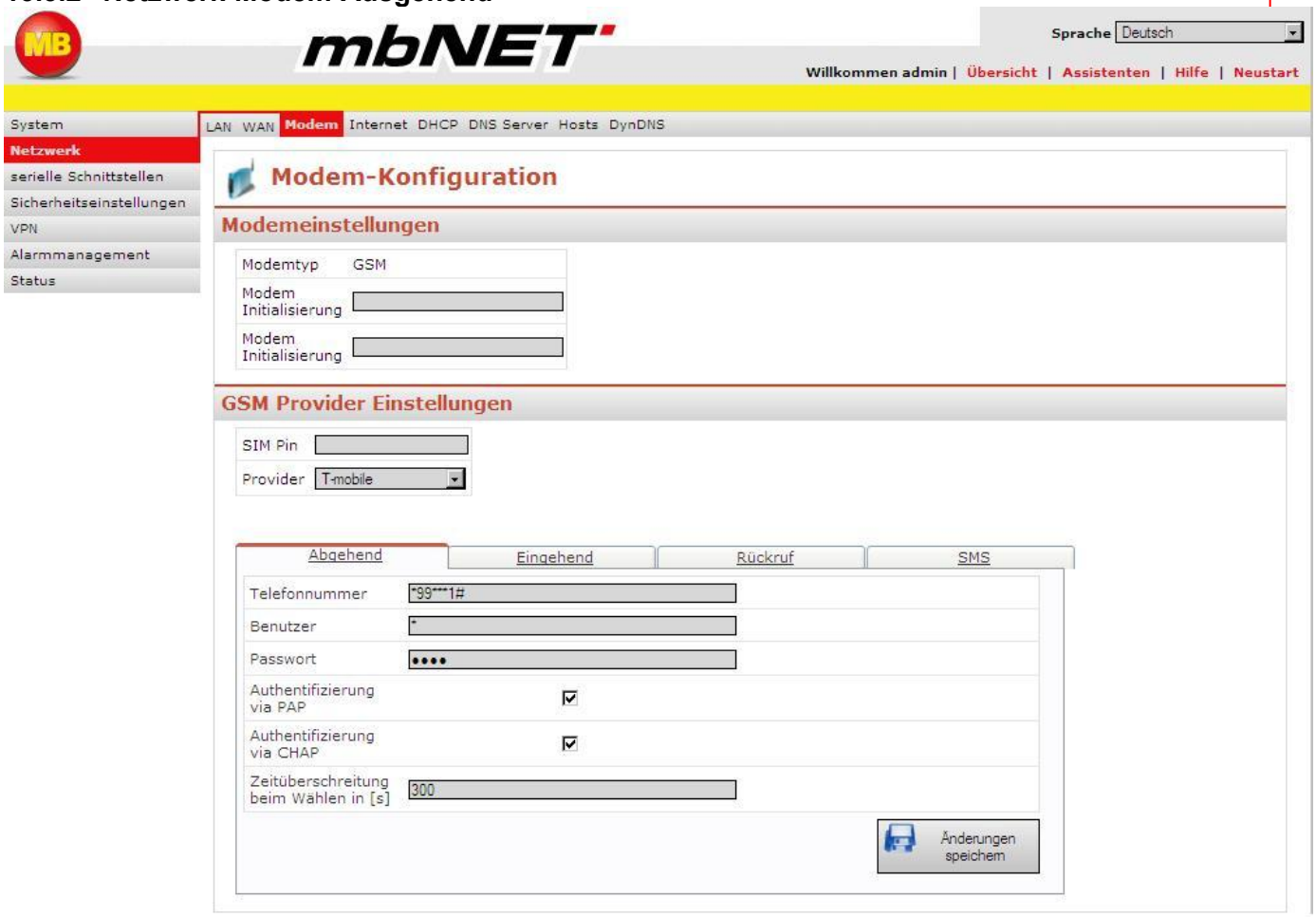


Abbildung 151

Die nachfolgenden Einstellungen beziehen sich auf abgehende Verbindungen des Modems

Bezeichnung	Beschreibung
Telefonnummer	Geben Sie hier die Rufnummer des entsprechenden Providers ein. Bei GSM-Modems lautet diese Nummer stets *99#
Benutzer	Geben Sie den Benutzernamen ein, der zur Einwahl beim entsprechenden Anbieter erforderlich ist. Weitere Infos hierzu erhalten Sie direkt bei ihrem Anbieter. Bei GSM-Modems finden sie z.B. unter http://www.mbconnectline.de/gsm/grps/gsm/grps.html weitere Informationen.
Passwort	Geben Sie das Passwort ein, das zur Einwahl beim entsprechenden Anbieter erforderlich ist. Weitere Infos hierzu erhalten Sie direkt bei ihrem Anbieter. Bei GSM-Modems finden sie z.B. unter http://www.mbconnectline.de/gsm/grps/gsm/grps.html weitere Informationen
Authentifizierung via PAP	Übernehmen Sie das standardmäßig eingestellte Authentifizierungsprotokoll. Dies ist bei der Einrichtung einer DFÜ-Verbindung grundsätzlich voreingestellt.
Authentifizierung via CHAP	Übernehmen Sie das standardmäßig eingestellte Authentifizierungsprotokoll. Dies ist bei der Einrichtung einer DFÜ-Verbindung grundsätzlich voreingestellt. CHAP ist im Regelfall das Verfahren, das bei der Anmeldung an den Internet-Zugang beim Internetdienstanbieter (ISP) per Modem oder ISDN-Adapter durchgeführt wird.
Zeitüberschreitung beim Wählen in [s]	Nach dieser eingestellten Zeit wird der Wählversuch abgebrochen und eine erneute Anwahl gestartet.

13.3.3 Netzwerk – Modem-Rückruf

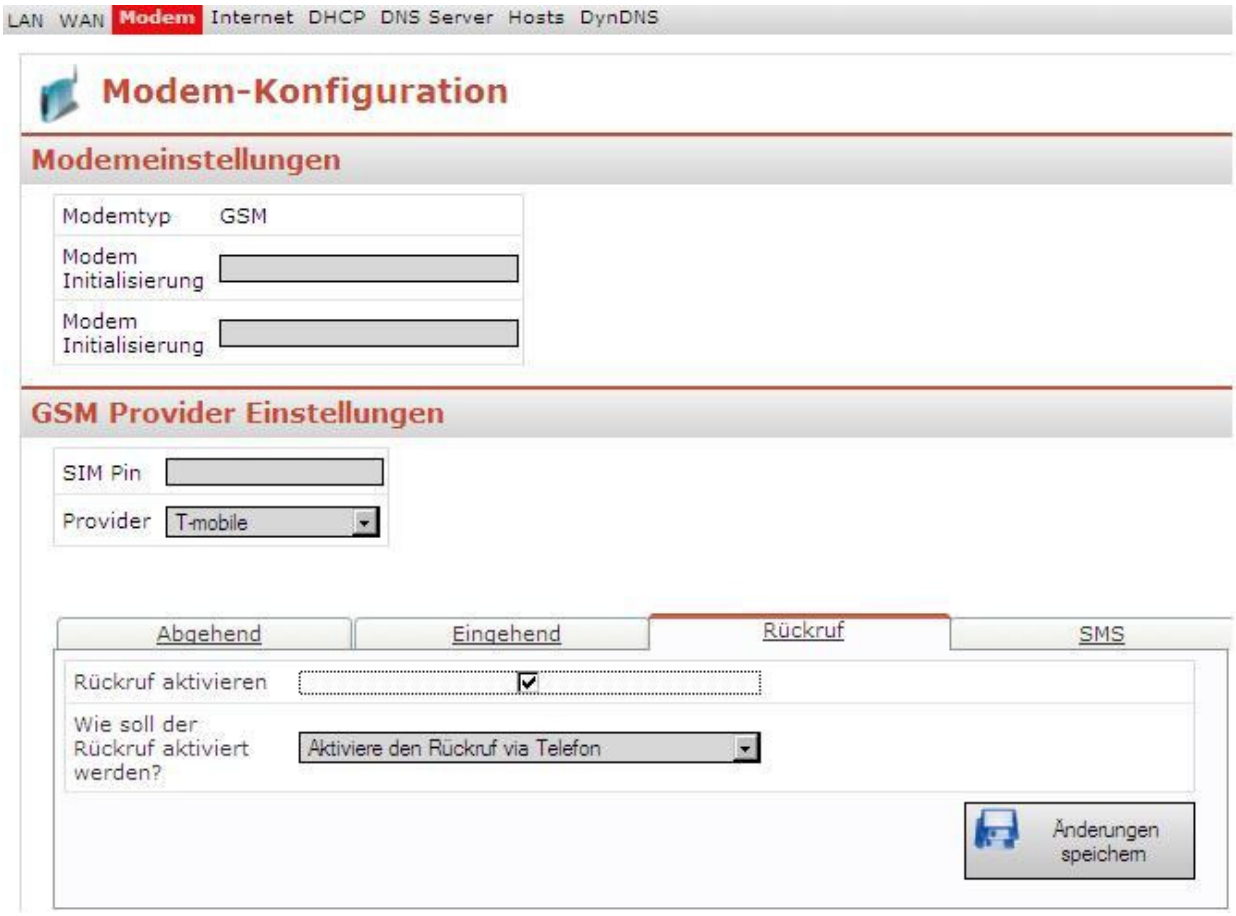


Abbildung 152

Die nachfolgenden Einstellungen beziehen sich auf die Rückruffunktion. Diese Funktion dient dazu, den Vorgang für die Einwahl ins Internet von außen durch einen Telefonanruf bzw. DFÜ-Verbindung zu starten. Es muss eingestellt werden, dass die Internetverbindung via WAN, oder via Modem aufgebaut wird. Damit die Rückruffunktion genutzt werden kann, muss das **mb*NET*** in den Wartezustand gebracht werden.

Bezeichnung	Beschreibung
Rückruf aktivieren	Wenn Sie diese Option markieren, können Sie den Rückruf ermöglichen.
Wie soll der Rückruf aktiviert werden?	**Aktiviere den Rückruf via Telefon:** Wenn Sie diese Einstellung wählen, verbindet sich das *mbNET* ins Internet, wenn es von einem Telefon angerufen wird. Damit die Verbindung aufgebaut werden kann, muss das mbNET mit viermaligen Klingeln darauf aufmerksam gemacht werden. Im Anschluss daran legt das mbNET auf und startet den Vorgang für eine Einwahl zum Internet. Dies kann bis zu 30-40 Sek. dauern. **Einloggen und Button klicken:** Wenn Sie diese Einstellung wählen, verbindet sich das *mbNET* ins Internet, wenn Sie eine DFÜ-Verbindung zu dem *mbNET* aufgebaut haben und auf der Benutzeroberfläche im Menü **System** - **Info** auf den Knopf Call Back drücken. Nachdem hat man 30 Sekunden Zeit um die DFÜ-Verbindung wieder zu trennen, denn danach baut das *mbNET* die Verbindung ins Internet auf.

13.3.4 Netzwerk-Modem-SMS

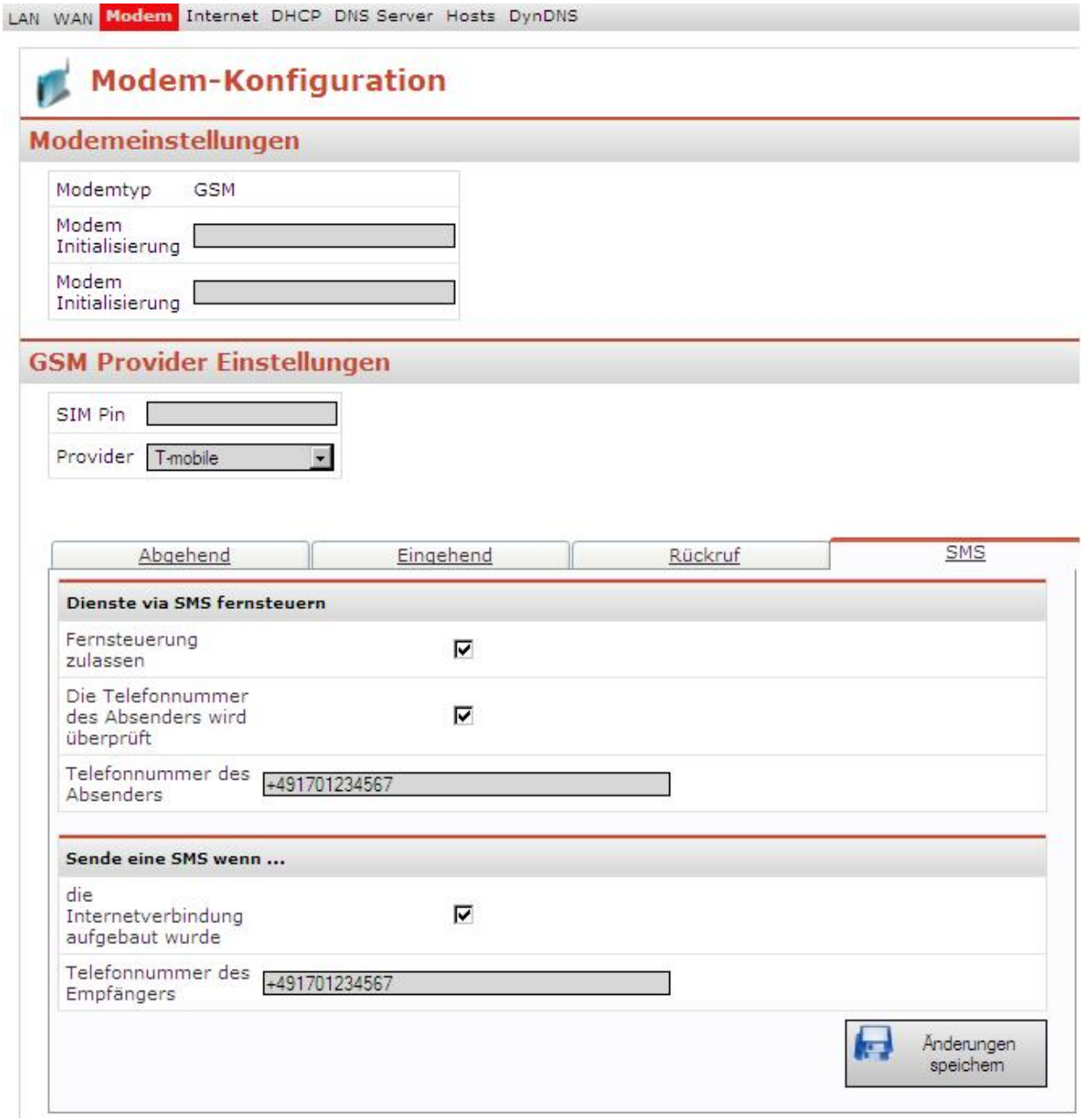


Abbildung 153

Bezeichnung	Beschreibung
Fernsteuerung zulassen	Mit dieser Funktion wird die Steuerung durch Kurznachrichten aktiviert
Die Tel. Nr. des Absenders wird überprüft	Hiermit wird sichergestellt, dass das mbNET nur Befehle per Kurznachrichten annimmt, die von einer bestimmten Nummer kommen. Jetzt müssen Sie noch die Telefonnummer des Absenders im Feld „Telefonnummer des Ab-senders“ direkt darunter eingeben. Kommen nun Befehle von einer anderen Nummer, dann werden diese abgewiesen.
SMS nutzen, wenn die Internetverbin-dung aufgebaut ist	Das mbNET kann Ihnen eine Kurznachricht zukommen lassen, sobald es sich mit dem Internet verbunden hatte. Zusätzlich müssen Sie im Feld darunter die Telefonnummer des Empfängers angeben.

Bitte beachten Sie, dass ihre Mobilfunknummern nicht mit der Null beginnen dürfen, sondern mit 49 (nur in Deutschland!).

13.4 Netzwerk - Internet

Für die Einwahl des Routers ins Internet ist dieser verbindungsspezifisch und abhängig von bestimmten Ereignissen entsprechend zu konfigurieren.

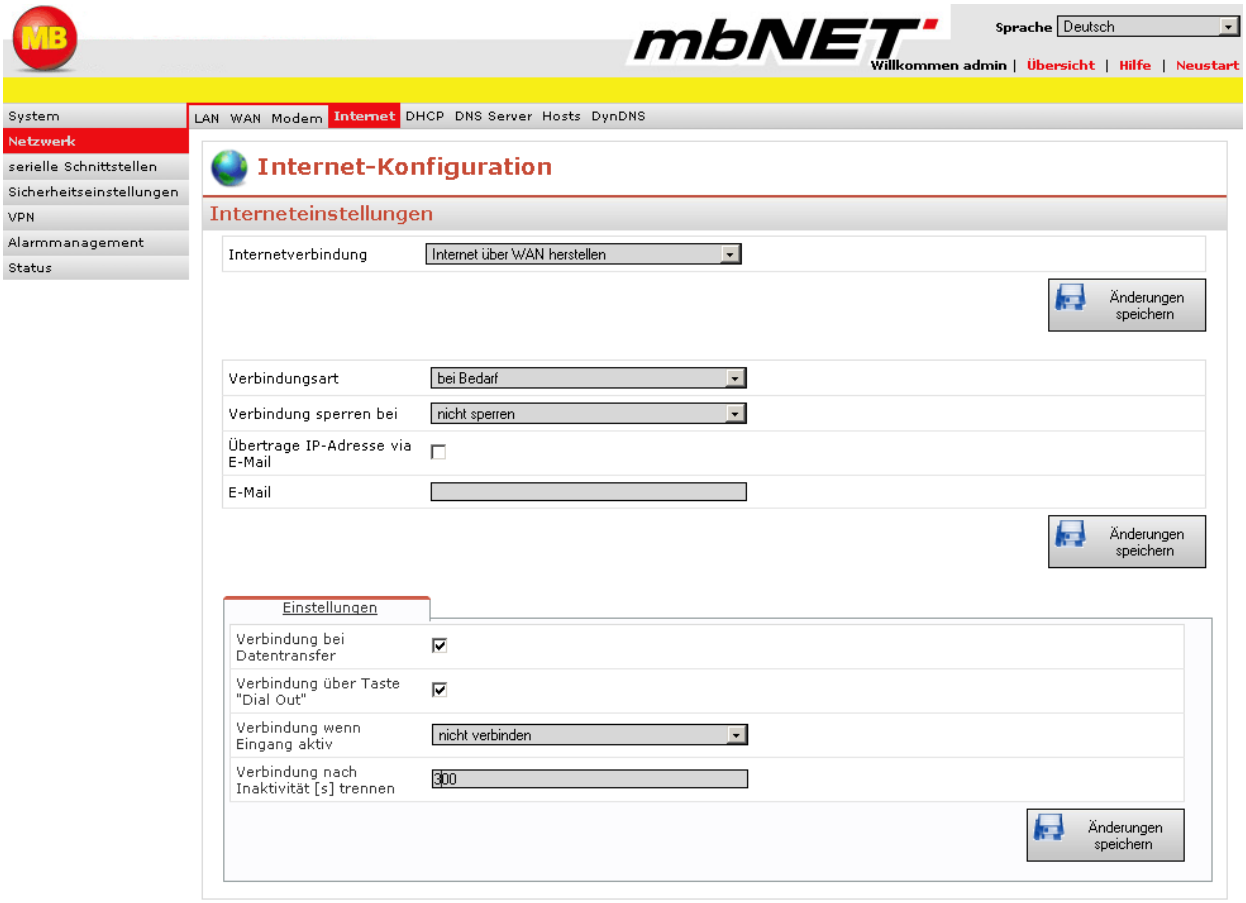


Abbildung 154

Bezeichnung	Funktion
Internetverbindung	Folgende Möglichkeiten stehen über das Auswahlfeld zur Verfügung: ❑ **Keine Verbindung** Wählen Sie diese Einstellung wenn das mbNET nicht selbst eine Internetverbindung herstellt. Das trifft z.B. zu, wenn in Ihrem Netzwerk bereits ein weiterer Router vorhanden ist, der für die Internetverbindung zuständig ist, oder wenn nur eine eingehende Wählverbindung über das öffentliche Telefonnetz erfolgt. ❑ **Internet über Modem herstellen** Bei dieser Einstellung wird eine Verbindung über Modem aufgebaut. Entsprechende Zugangsdaten sind bei den Einstellungen **Netzwerk – Modem** einzutragen. ❑ **Internet über WAN herstellen** Wenn die Internetverbindung z.B. über ein DSL-Modem erfolgen soll, dann ist diese Einstellung auszuwählen. Sie müssen jedoch zusätzlich unter **Netzwerk – WAN** ihre Internetzugangsdaten eingeben. Starten Sie danach das mbNET neu, damit die Änderungen wirksam werden.

Netzwerk - Internet (Fortsetzung)

Bezeichnung	Beschreibung
Verbindungsart	❑ **Verbindung immer aufrechterhalten** Wählen Sie diese Einstellung, wenn der Router beim Neustart oder durch Betätigen des Tasters **RESET** an der Frontseite des Routers sofort versucht eine Verbindung ins Internet herzustellen. **Achtung! Die Internet-Verbindung wird nicht getrennt** ❑ **Bei Bedarf** Wählen Sie diese Einstellung, wenn der Router dann eine Verbindung ins Internet aufbauen soll, wenn eine oder mehrere der nachfolgend aufgelisteten Optionen ausgewählt sind: ○ Verbindung ins Internet durch Betätigen der Taste **Dial out** ○ Verbindung ins Internet durch ein Signal an einen der Eingänge **E1,E2,E3** oder **E4** ○ Verbindung bei Datentransfer
Verbindung sperren bei	❑ **Nicht sperren:** Wählen Sie diese Option, wenn Sie möchten dass eine bestehende Internetverbindung nicht durch ein Eingangssignal an einem digitalen Eingang getrennt werden kann. ❑ **Eingang1, Eingang2, Eingang3, Eingang4:** Wählen Sie diese Option, wenn eine bestehende Internetverbindung durch ein Signal an einem der ausgewählten digitalen Eingänge unterbrochen werden soll.
Übertrage IP-Adresse via E-Mail	Hier können Sie einstellen, ob eine Email mit der aktuellen öffentlichen IP-Adresse an eine vorher eingetragene Adresse gesendet werden soll.
EMail	Falls die Option „IP via Email versenden“ gewählt wurde ist hier ihre EMail-Adresse angegeben. Sie können sie aber auch manuell in diesem Feld eintragen.
Einstellungen	Die Registerkarte **Einstellungen** ist nur dann sichtbar, wenn eine Verbindung zum Internet entweder über WAN oder per Modem ausgewählt wurde, und die Verbindungsart **Bei Bedarf** über das Auswahlfeld eingestellt ist. Die nachfolgenden Einstellungsmöglichkeiten werden angezeigt:
Verbindung bei Datentransfer	Soll eine Verbindung ins Internet durch gesendete Datenpakete stattfinden, dann ist das Kästchen mit einem Häkchen zu versehen. D.h. wenn vom LAN aus versucht wird, einen Teilnehmer zu erreichen, der sich nicht im LAN befindet, dann wird eine Verbindung ins Internet aufgebaut.
Verbindung über Taste “Dial-out“	Soll die Verbindung ins Internet durch Drücken des Tasters **Dial out** an der Gerätefront ausgelöst werden, dann versehen Sie das Kästchen mit einem Häkchen.
Verbindung wenn Eingang aktiv	❑ **Nicht verbinden** Wählen Sie diese Option, wenn Sie möchten, dass eine Internetverbindung nicht durch ein digitales Signal an einem der Eingänge ausgelöst werden kann. ❑ **Eingang1, Eingang2, Eingang3, Eingang4** Wählen Sie diese Option, wenn eine Internetverbindung durch ein Signal am entsprechenden Eingang aufgebaut werden soll.
Verbindung nach Inaktivität [s] trennen	Hiermit stellen Sie ein, nach welcher Zeit die bestehende Internetverbindung getrennt werden soll, sobald keine Datenpakete mehr vom Router versandt werden. Keine Eingabe schaltet diese Funktion aus.

13.5 Netzwerk - DHCP

Der Industrierouter kann als DHCP-Server im LAN oder WAN-Netzwerk konfiguriert werden. Durch DHCP ist die Einbindung eines neuen Computers in ein bestehendes Netzwerk ohne weitere Konfiguration möglich. Es muss lediglich der automatische Bezug der IP-Adresse am Computer eingestellt werden.

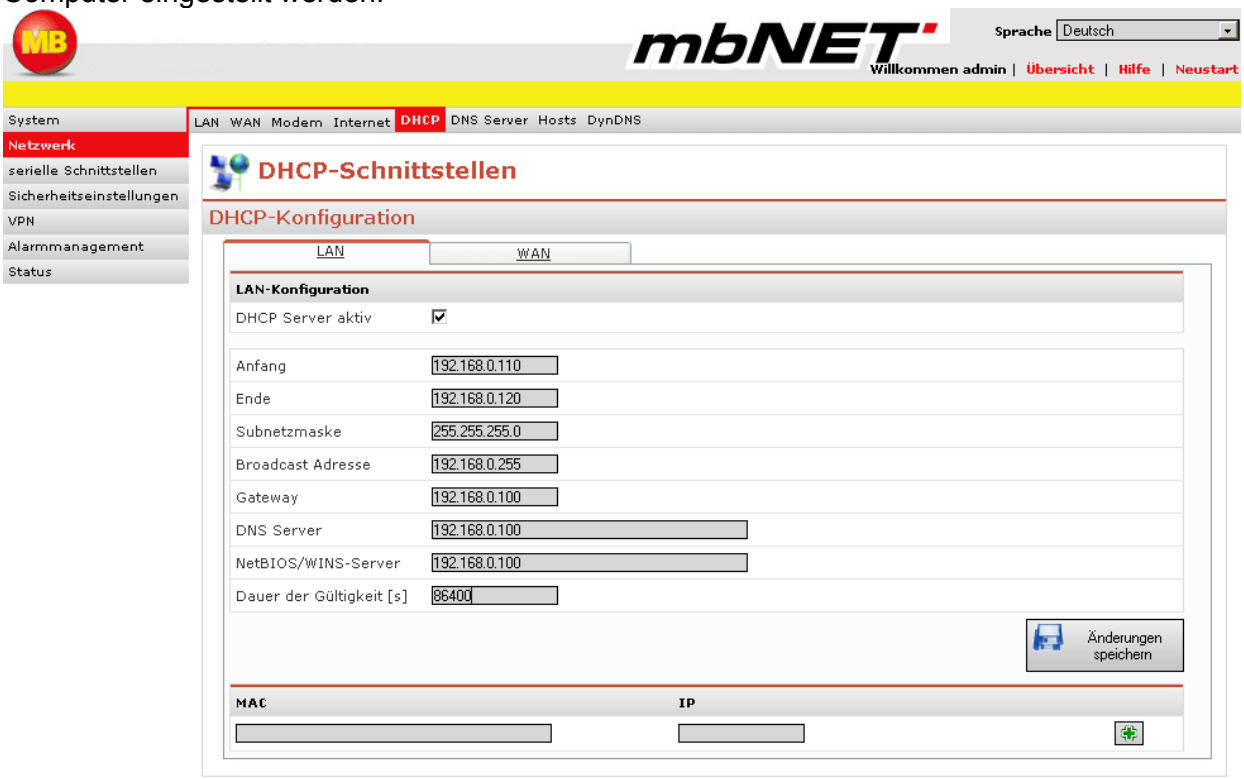


Abbildung 155

Bezeichnung	Funktion
LAN / WAN	Auswahl zur Konfiguration der LAN bzw. WAN-Schnittstelle.
DHCP-Server aktiv	Durch markieren der Funktion kann der Router als DHCP-Server an der entsprechenden Schnittstelle aktiviert werden.
Anfang	Hier ist die Anfangsadresse des Adressbereichs einzugeben, der vom DHCP-Server verwaltet wird.
Ende	Endadresse des vom DHCP-Server verwalteten Bereichs.
Subnetzmaske	Subnetzmaske des vom DHCP-Server verwalteten Bereichs.
Broadcast Adresse	Broadcastadresse des vom DHCP-Server verwalteten Bereichs.
Gateway	Optionale Eingabe. Hier kann die Adresse eines Routers eingetragen werden, der die im Netzwerk anwesenden Clients mit dem Internet oder mit einem anderen Netzwerk verbindet. Tragen Sie hier die LAN IP-Adresse des Routers ein.
DNS-Server	Optionale Eingabe eines im Netzwerk vorhandenen DNS-Servers. Tragen Sie hier die LAN IP-Adresse des Routers ein.
NetBIOS/WINS-Server	Optionale Eingabe eines im Netzwerk vorhandenen NetBIOS/WINS-Servers.
Dauer der Gültigkeit [s]	Zeitdauer während ein Client von einem DHCP-Server eine bestimmte IP-Adresse zugeteilt bekommt.
Tabelle MAC / IP	Tragen Sie hier die feste Zuordnung zwischen IP-Adresse und MAC-Adresse ein. D.h. sie können hier vorgeben, dass ein Gerät mit einer bestimmten MAC-Adresse immer dieselbe Adresse erhält.

13.6 Netzwerk - DNS-Server

Mit Hilfe von DNS werden IP-Adressen in Namen umgesetzt.
Werksseitig ist der Industrierouter so konfiguriert, dass der DNS-Server vom Internetservice-provider vergeben wird. Bei einer dauerhaften Verbindung des Industrierouters kann hier ein eigener DNS-Server hinzugefügt werden. Dieser wird dann vor dem vom Internetserviceprovi-der vergebenen Server verwendet.

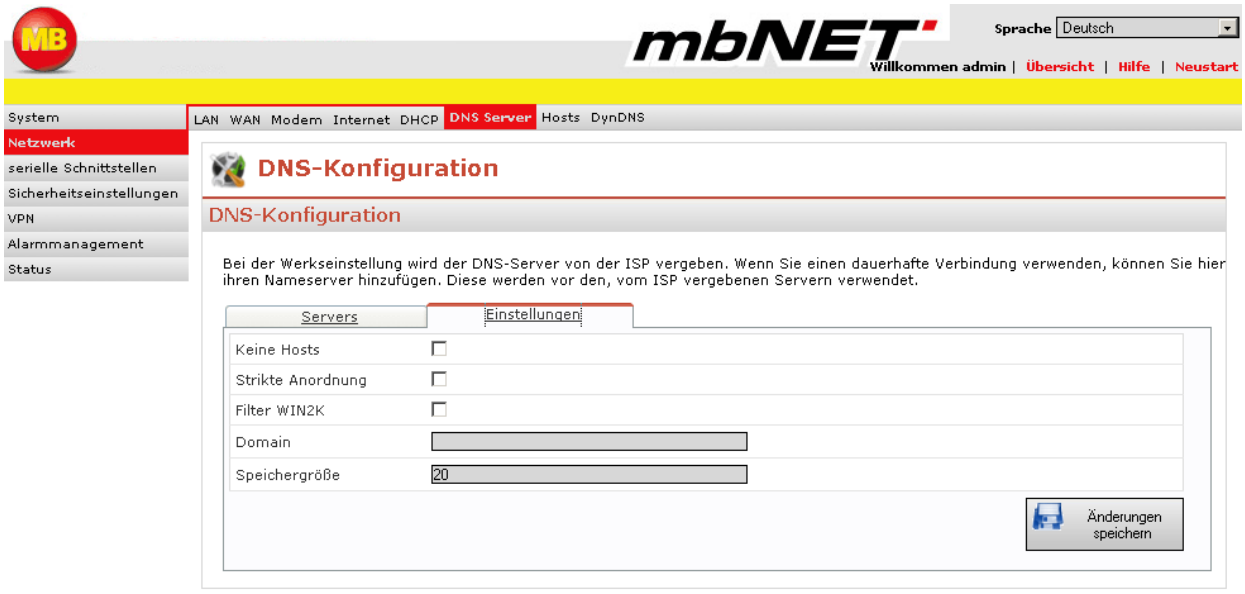


Abbildung 156

Bezeichnung	Funktion
Servers	Nach Anklicken dieser Registerkarte kann ein entsprechender DNS-Server ein-getragen werden.
Einstellungen	Nach Anwahl dieser Registerkarte können die nachfolgend aufgelisteten Ein-stellungen bezüglich DNS-Server aktiviert bzw. eingetragen werden.
Keine Hosts	Die unter Netzwerk-Hosts eingetragenen Computernamen werden nicht be-rücksichtigt.
Strikte Anordnung	Es wird genau die Reihenfolge der Einträge wie unter „Servers“ eingehalten.
Filter WIN2K	Filtert ständige und unnötige Anfragen von Windows-Clients. Bei einer Internet-verbindung „Bei Bedarf“ ist diese Einstellung sinnvoll, dann wird nicht immer ei-ne Internetverbindung bei jeder Anfrage aufgebaut.
Domain	Sie können hier ein sogenanntes Domain-Suffix eintragen.
Speichergröße	Geben Sie hier Anzahl der gespeicherten Namen an. D.h. wie viel Namen mit IP-Adresse zwischengespeichert werden.

13.7 Netzwerk - Hosts

Über diese Einstellung können immer genau einer IP-Adresse ein bestimmter Name zugeordnet werden, um DNS-Anfragen direkt beantworten zu können. Über die Eingabefelder können IP-Adresse und zugehöriger Name eingetragen und abgespeichert, bzw. gelöscht werden. Das mbNET muss somit nicht einen anderen DNS-Server befragen, sondern beantwortet die Anfrage direkt.

Abbildung 157

13.8 Netzwerk - DynDNS

13.8.1 Allgemeines

Da der Industrierouter bei einer Einwahl ins Internet eine eindeutige IP zugewiesen bekommt, kann er von einem Client-PC anhand dieser IP gefunden werden. Sobald er aber wieder die Verbindung ins Internet unterbricht und später wieder neu einwählt, erhält er eine neue IP-Adresse. Der DynDNS–Dienst dient dazu, den Industrierouter immer unter dem gleichem Namen erreichen zu können. Er dient zur Umsetzung von Adressen in Namen und umgekehrt.

Weitere Dienste:
ez-ip: www.EZ-IP.Net
dyndns: www.dyndns.org
ods: www.ods.org
tzo: www.tzo.com
easydns: www.easydns.com
justlinux v1.0 (penguinpowered): www.penguinpowered.com
justlinux v2.0 (penguinpowered): www.justlinux.com
dyns: www.dyns.cx
zoneedit: www.zoneedit.com
heipv6tb: www.he.net
dyndns-static: www.dyndns.org
dyndns-custom: www.dyndns.org
easydns-partner: www.easydns.com
dhs: www.dhs.org

13.8.2 Vorgehensweise zur Einrichtung der DynDNS-Konfiguration

Ab der Firmware Version 1.4.0 steht ein automatischer DynDNS Dienst bereit. Dieser DynDNS Dienst wird von MB Connect Line betrieben. *Eine Anmeldung bzw. Registrierung ist nicht erforderlich.*

Um einen öffentlichen DynDNS Dienst nutzen zu können, müssen Sie sich zunächst registrieren. Diese Registrierung ist in der Regel kostenlos und sollte keine größeren Schwierigkeiten bereiten.

Sofern Sie für einen vom Industrierouter unterstützten DynDNS-Dienst registriert sind, können Sie die Eingaben in der nachfolgenden Bildschirmmaske eintragen bzw. auswählen.

Wählen Sie **Netzwerk** – **DynDNS**
Es erscheint daraufhin die folgende Bildschirmmaske:

Netzwerk - DynDNS (Fortsetzung)

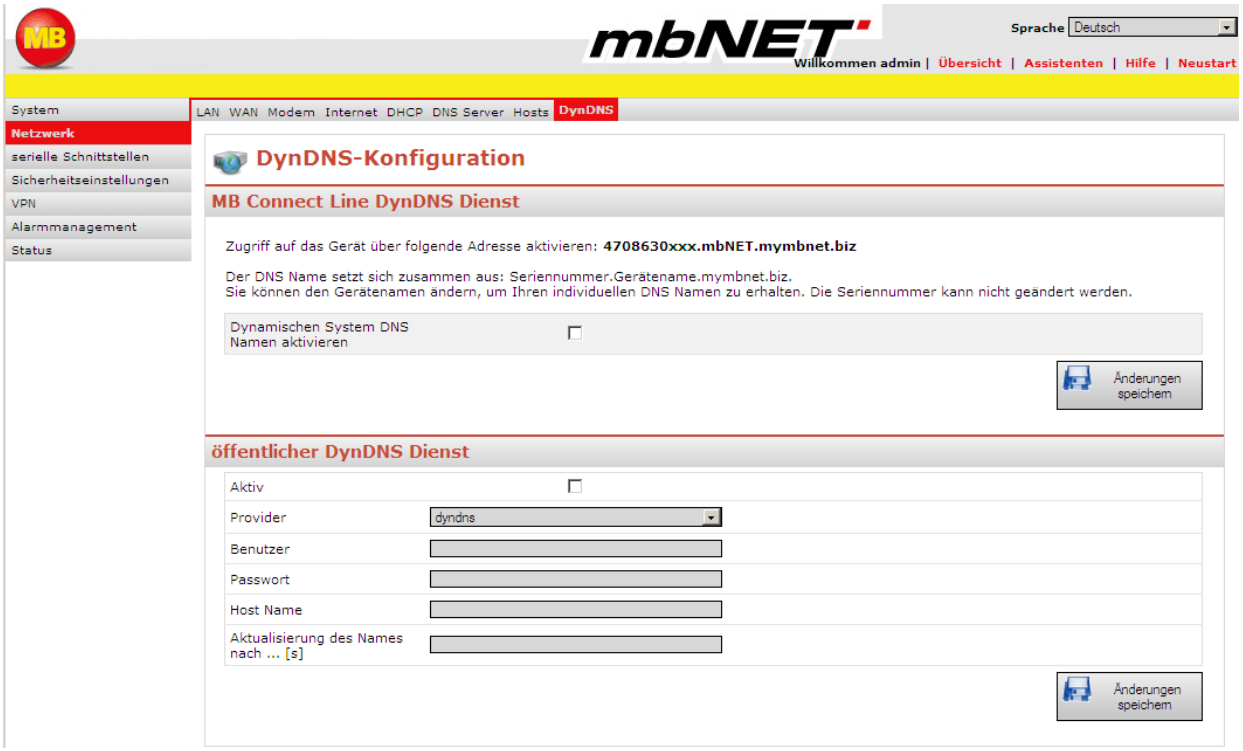


Abbildung 158

MB Connect Line DynDNS Dienst	
Bezeichnung	**Beschreibung**
Dynamischen System DNS Namen aktivieren	Diese Option aktiviert den automatischen DynDNS Dienst von MB Connect Line. Der Namensaufbau ist in diesem Fall fest vorgegeben und kann nur an einer Stelle frei definiert werden: Name: Seriennummer.Gerätename.mymbnet.biz Die Seriennummer ist fix und der Gerätename ist frei wählbar. Beispiel: Gerätename: mbNET600 Seriennummer: 123456789 = Name im Internet: „123456789.mbNET600.mymbnet.biz“ ca. 1-2 Minuten nach Einwahl ins Internet, ist der Name weltweit verfügbar.

Öffentlichen DynDNS Dienst	
Bezeichnung	**Beschreibung**
Aktiv	Wenn Sie beim DynDNS-Anbieter entsprechend registriert sind und der Industrierouter diesen Service nutzen soll, dann klicken Sie auf die Checkbox um diese mit einem Häkchen zu versehen. Der Industrierouter meldet somit bei der nächsten Einwahl ins Internet die aktuelle IP-Adresse die er vom Internet-Service-Provider erhalten hat an den DynDNS-Service.
Provider	Wählen Sie hier über das Auswahlfeld den Namen des Anbieters aus, bei dem Sie registriert sind, z.B. DynDNS.
Benutzer	Geben Sie den Benutzernamen ein, den Sie beim DynDNS-Dienst bei der Registrierung eingegeben haben.
Passwort	Geben Sie das Passwort ein, das Sie beim DynDNS-Dienst bei der Registrierung eingegeben haben.
Host Name	Geben Sie hier den Namen den Sie beim DynDNS-Dienst für den Industrierouter eingegeben haben.
Aktualisierung des Namens nach ....[s]	Immer wenn sich die IP-Adresse des Industrierouters ändert, z.B. nach erneuter Einwahl ins Internet. Geben Sie hier die Zeit ein, nach der der Industrierouter den DynDNS-Anbieter über die neue IP-Adresse informiert.

14. Serielle Schnittstellen

14.1 Allgemeines

Bei bekannter IP-Adresse kann über eine Einwahlverbindung oder über das Internet auf die beiden seriellen Schnittstellen zugegriffen werden.

Die serielle Schnittstelle **COM1** kann direkt über die Weboberfläche auf **RS232**, **RS485** und **RS422** konfiguriert werden und die entsprechenden Steuerbefehle z.B. an die angeschlossene Steuerung oder angeschlossenes Gerät weiterleiten.

Abhängig von der Gerätevariante ist die Schnittstelle **COM2** bei einer Gerätevariante als MPI/Profibus-Schnittstelle, bei der anderen Gerätevariante wie **COM1** ausgeführt. Mit der MPI/Profibus-Schnittstelle ist es möglich von der Ferne aus auf Steuerungen z.B. S7-300/400 zuzugreifen. Die MPI/PROFIBUS Schnittstelle unterstützt Baudraten bis 12Mbit/s.

Nach Betätigen der Schaltfläche **Serielle Schnittstellen** wird die folgende Bildschirmmaske angezeigt:

Serielle Schnittstellen (Fortsetzung)

Abbildung 159

Bezeichnung	Funktion
COM 1	Auswahl zur Konfiguration der Schnittstelle COM1 Die nachfolgenden Einstellungen betreffen nur diese Schnittstelle.
Schnittstellentyp	Über das Auswahlfeld stellen Sie hiermit den Schnittstellentyp COM1 ein. Folgende Typen stehen zur Auswahl: RS232, RS485 2-Draht, RS485 4-Draht, RS422
Treiber	Entweder wählen Sie einen der Treiber aus der Liste oder geben die Schnittstellenparameter selbst vor
Treiber	Wählen Sie den zu ladenden Gerätetreiber aus.Es stehen die folgenden Gerätetreiber folgender Firmen zur Auswahl: AllanBradley, AMK, ASB, AtlasCopco, Baumüller, Berger, Bosch, B&R, DanfossVLT, Elau, F-Tron,GE_Fanuc, Hitachi, I-for-T, Indramal, IQ2000, KEB; Kuhnke, KEB, Lauer, Lenze, Locon, Micro_Innovation, Mitshubishi, Möller, Motoman, Npos, Omron, Parker Hauser CompaxC3, Phoenix, Pilz, PLC Direct, Primo, Proface, Promicon, Quin, SCS Automata, Seidel Kollmorgen, SEW, Siemens, Stoeber, Stromag, Sütron, Tsx37, Tsx47, Tsx57, Vectron, Vega Sensor, Voelkel Grenzlastregler, Winloc
Protokoll	Wählen Sie das Protokoll über das die Kommunikation zum angeschlossenen Gerät aufgenommen wird. Zur Auswahl stehen:TCP und UDP
Port	Tragen Sie hier den Port ein, über den die Kommunikation stattfinden soll.
Ports in Firewall freischalten	Ist diese Checkbox aktiviert, wird der oben angegeben Port in der Firewall freigeschalten und Sie können über die öffentliche Adresse auf die seriellen Geräte zugreifen

Serielle Schnittstellen (Fortsetzung)

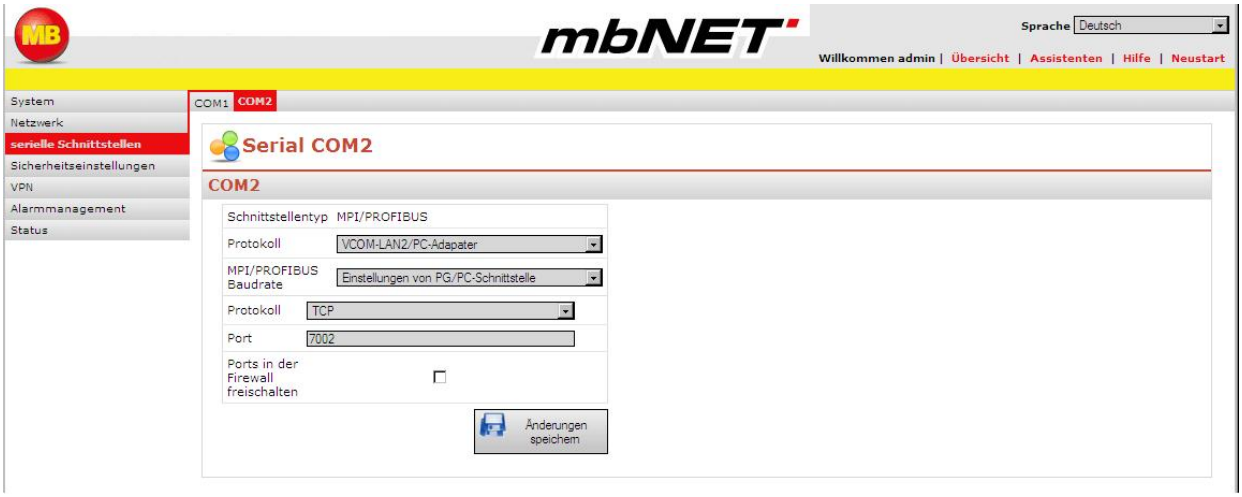


Abbildung 160

Bezeichnung	Funktion
COM2	Auswahl zur Konfiguration der Schnittstelle COM2 sog. MPI-Profibus-Schnittstelle. Die nachfolgenden Einstellungen betreffen nur diese Schnittstelle.
Schnittstel-lentyp	MPI-Profibus-Schnittstelle oder Serielle Schnittstelle (wie bei COM1).
Protokoll	Über die VCOM-LAN2 kann mit dem mbNET gearbeitet werden, wie mit einem PC-Adapter. Sie müssen keine Änderungen vornehmen.
MPI/Profibus-Baudrate	Wählen Sie unter folgenden Optionen aus: Einstellungen von PG/PC-Schnittstelle, 3Mbit/s, 6Mbit/s und 12Mbit/s
Protokoll	Wählen Sie das Protokoll über das Kommunikation zum angeschlossenen Gerät aufgenommen wird. Zur Auswahl stehen: TCP und UDP
Port	Tragen Sie hier den Port ein, über den die Kommunikation stattfinden soll.
Ports in der Firewall frei-schalten	Ist diese Checkbox aktiviert, wird der oben angegeben Port in der Firewall freige-schalten.

Ab Firmware 2.0 wird die LED RxD2 angeschaltet wenn eine MPI-/ bzw. PROFIBUS-Verbindung aufgebaut ist und die LED TxD2 blinkt bei Datenverkehr.

14.2 Serielle Schnittstellen auf Ihrem PC umleiten (VCOM LAN2)

Um die seriellen Schnittstellen (auch MPI/PROFIBUS) des Routers auf Ihrem Client-PC verfügbar zu haben, benötigen Sie das Softwaretool VCOM LAN2. VCOM LAN2 kann kostenlos von der WEB-Seite www.mbconnectline.de geladen werden. VCOM LAN2 stellt auf Ihrem Client-PC zwei virtuelle COM-Schnittstellen dar. Über diese virtuellen COMs werden dann die Daten ausgetauscht.

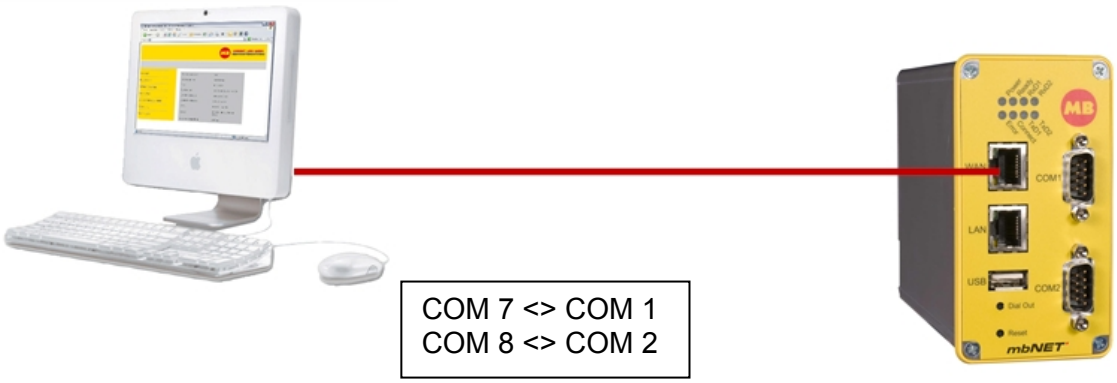


Abbildung 161

Sie müssen die VCOM LAN2 Setup-Datei ausführen und den Installationsanweisungen folgen. Es ist bei der Einstellung einer Anlage darauf zu achten, dass die Ports (**TCP je nach Einstellung / UDP 25400 und 25401**) auf der Seite des Client-PCs und auf der Seite des Industrierouters freigeschaltet sind. Es ist weiterhin zu beachten, dass wenn Sie „Verbindung erst aufbauen, wenn virtueller COM-Port von einem Programm geöffnet wird“ als Verbindungseinstellung wählen, dass ein paar Daten verloren gehen können, bis der virtuelle COM-Port geöffnet wird, da einige Programme sofort Daten an den COM-Port schicken, bevor der virtuelle COM-Port eine Verbindung aufgebaut hat.
Weitere Informationen zur VCOM LAN2 können Sie danach der Programmhilfe entnehmen.

14.2.1 Einstellungen zu Simatic Manager

Wenn Sie die Verbindung zu einer Steuerung von Siemens aufbauen möchten, dann müssen Sie vorher prüfen ob im Simatic Manager unter

Extras → PG/PC-Schnittstelle einstellen → PC-Adapter (PROFIBUS) oder PC-Adapter (MPI)

auswählen und auf Knopf „Eigenschaften“ drücken. Daraufhin öffnet sich ein Menüfenster mit dem Reiter „Lokaler Anschluß“. Dort bei Übertragungsgeschwindigkeit **M U S S** 38400 eingetragen sein.

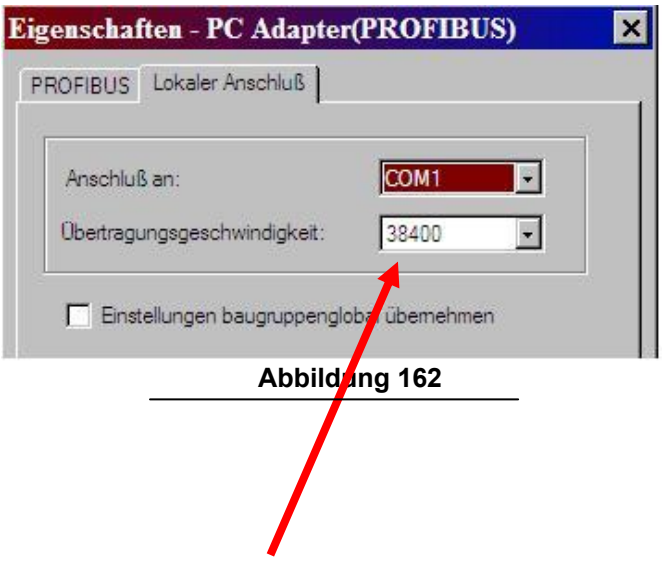


Abbildung 162

15. Sicherheitseinstellungen

15.1 Allgemeines

Zum Schutz vor fremden und unberechtigten Zugriffen bzw. Verbindungsversuchen besitzt der Industrierouter eine integrierte Firewall. Über diese Firewall wird der kommende und gehende Datenverkehr kontrolliert, protokolliert und freigegeben bzw. gesperrt.

Die Firewall kann allgemein in einer der drei folgenden Varianten konfiguriert werden:

- **Maximalste Sicherheitsstufe**
  Die entsprechenden Freigaben für den Datenverkehr müssen entsprechend konfiguriert werden. Sowohl der eingehende und ausgehende Datenverkehr ist gesperrt.
  Für den Zugriff auf die Weboberfläche (von außen!) muss **TCP-Protokoll** und der **Ziel-Port 80** bei den Regeln **WAN >LAN** eingetragen und aktiviert werden. Starten Sie jedoch eine VPN-Verbindung, dann wird der Zugriff dementsprechend für die Datenpakete aus dem VPN-Tunnel freigegeben.

- **Normale Sicherheitsstufe**
  Bei dieser Variante wird der eingehende Datenverkehr (Daten vom Internet) gesperrt, während die ausgehenden Daten akzeptiert werden.

- **Minimalste Sicherheitsstufe**
  Bei dieser Variante werden alle ein- und ausgehenden Daten akzeptiert.

Die Variante Minimalste Sicherheitsstufe sollte nur zu Testzwecken kurzzeitig eingestellt werden, da jeglicher Datenverkehr und Zugriff von außen möglich ist!

Sicherheitseinstellungen (Fortsetzung)

15.2 WAN>LAN

Über diese Einstellung wird der eingehende Datenverkehr geregelt, d.h. die nachfolgend aufgeführten Einstellungen gelten nur für den von außen eingehenden Datenverkehr.

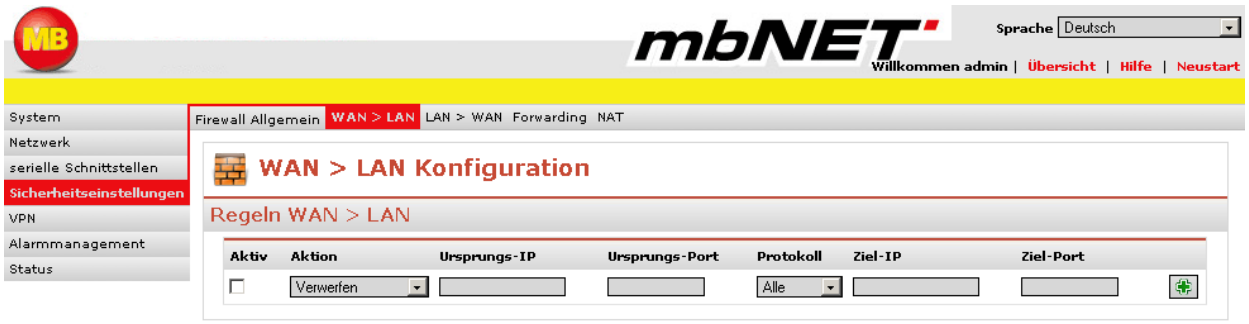


Abbildung 163

Bezeichnung	Beschreibung
Aktiv	Versehen Sie die Checkbox durch Anklicken mit einem Häkchen damit die nachfolgenden Einstellungen nach dem Speichern aktiviert werden.
Aktion	Folgende Optionen stehen zur Auswahl: **Verwerfen:** Wird diese Option gewählt, dann dürfen keine Datenpakete passieren. Der Absender erhält hierbei keine Information über deren Verbleib. **Abweisen:** Bei dieser Option werden die Datenpakete zurückgewiesen. Der Absender erhält eine Information darüber, dass die Datenpakete zurückgewiesen wurden. **Akzeptieren:** Hier dürfen die Datenpakete passieren.
Ursprungs-IP	Tragen Sie hier die IP ein, für deren eingehende Datenpakete eine der eingestellten Aktionen ausgeführt werden soll. Lässt man das Feld frei, gilt die eingestellte Aktion für alle IP-Adressen.
Ursprungs-Port	Tragen Sie hier den Port ein über den die Datenpakete eingehen.
Protokoll	Folgende Möglichkeiten stehen zur Auswahl: **Alle**:Die eingestellte Regel gilt für alle Protokolle **tcp**: Die eingestellte Regel gilt nur für das TCP-Protokoll **udp**: Die eingestellte Regel gilt nur für das UDP-Protokoll **icmp**: Die eingestellte Regel gilt nur für das ICMP-Protokoll
Ziel-IP	Tragen Sie hier die IP ein, an die die Datenpakete weitergeleitet werden sollen.
Ziel-Port	Tragen Sie den Port ein, über den die Datenpakete weitergeleitet werden.
	Editieren der Einstellungen in der aktuellen Zeile.
	Eingaben in der momentanen Zeile löschen.
	Aufnahme einer neuen Regel.
	Temporäres Speichern der angelegten Regel.
	Ändert die Reihenfolge der angelegten Regeln.

15.3 LAN>WAN

Über diese Einstellung wird der ausgehende Datenverkehr geregelt, d.h. die nachfolgend aufgeführten Einstellungen gelten nur für den von außen eingehenden Datenverkehr.

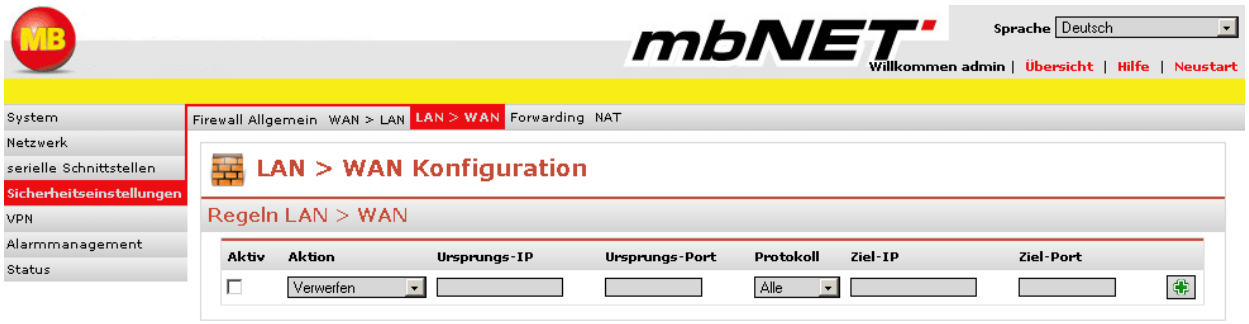


Abbildung 164

Bezeichnung	Beschreibung
Aktiv	Versehen Sie die Checkbox durch Anklicken mit einem Häkchen damit die nachfolgenden Einstellungen nach dem Speichern aktiviert werden.
Aktion	Folgende Optionen stehen zur Auswahl: **Verwerfen:** Wird diese Option gewählt, dann dürfen keine Datenpakete passieren. Der Absender erhält hierbei keine Information über deren Verbleib. **Abweisen:** Bei dieser Option werden die Datenpakete zurückgewiesen. Der Absender erhält eine Information darüber, dass die Datenpakete zurückgewiesen wurden. **Akzeptieren:** Hier dürfen die Datenpakete passieren.
Ursprungs-IP	Hier wird die IP eines Rechners eingetragen von dem aus Datenpakete ins Internet geschickt werden. Lässt man das Feld frei, gilt die eingestellte Aktion für alle IP-Adressen.
Ursprungs-Port	Hier den Port eingeben über den die Datenpakete ins Internet gehen.
Protokoll	Folgende Möglichkeiten stehen zur Auswahl: **Alle**:Die eingestellte Regel gilt für alle Protokolle **tcp**: Die eingestellte Regel gilt nur für das TCP-Protokoll **udp**: Die eingestellte Regel gilt nur für das UDP-Protokoll **icmp**: Die eingestellte Regel gilt nur für das ICMP-Protokoll
Ziel-IP	Tragen Sie hier die Zieladresse der Datenpakete im Internet ein.
Ziel-Port	Tragen Sie hier den Port ein, über den die Datenpakte zur Ziel-IP geschickt werden.
	Editieren der Einstellungen in der aktuellen Zeile.
	Eingaben in der momentanen Zeile löschen.
	Aufnahme der neuen Regel und temporäres Abspeichern.
	Temporäres Speichern der angelegten Regel.
	Ändert die Reihenfolge der angelegten Regeln.

Sicherheitseinstellungen (Fortsetzung)

15.4 Forwarding

Über diese Einstellung werden Anfragen von bestimmten IP-Adressen und Ports wiederum an definierte IP-Adressen und Ports weitergeleitet.

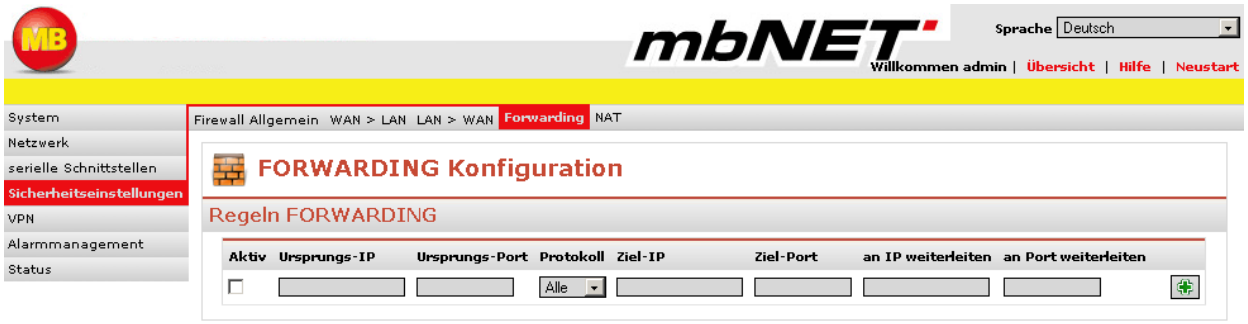


Abbildung 165

Bezeichnung	Beschreibung
Aktiv	Versehen Sie die Checkbox durch Anklicken mit einem Häkchen damit die nachfolgenden Einstellungen nach dem Speichern aktiviert werden.
Ursprungs-IP	Hier können Sie die IP eintragen, von der Datenpakete empfangen werden. Wird hier ein Eintrag vorgenommen, werden nur Pakete von dieser einen Adresse weitergeleitet.
Ursprungs-Port	Hier können Sie den Port angeben, über den die Datenpakete eingehen. Wird hier ein Eintrag vorgenommen, dann werden nur Pakete die speziell über diesen Port geschickt werden weitergeleitet.
Protokoll	Folgende Protokolle stehen zur Auswahl: **Alle**: Die eingestellte Regel gilt für alle Protokolle **tcp**: Die eingestellte Regel gilt nur für das TCP-Protokoll **udp**: Die eingestellte Regel gilt nur für das UDP-Protokoll
Ziel-IP	Hier die IP eintragen, an die die Datenpakete ursprünglich gesendet werden sollen.
Ziel-Port	Hier den Port angeben, über den die Datenpakete zur Ziel-IP gesendet werden.
an IP weiterleiten	Hier die IP eintragen, an die die Datenpakete tatsächlich weitergeleitet werden
an Port weiterleiten	Hier den Port angeben, über den die Datenpakete tatsächlich weitergeleitet werden.
	Aufnahme der neuen Einstellungen und temporäres Abspeichern.

Sicherheitseinstellungen (Fortsetzung)

15.5 NAT

Über diese Einstellung ist es möglich zwei Netzwerke die im gleichen Adressbereich liegen trotzdem miteinander zu verbinden. Wenn zum Beispiel ein Netzwerk mit der Adresse 192.168.0.0/24 mit einem Netzwerk mit der gleichen Adresse verbunden werden soll, so ist das nur möglich, wenn eines der beiden Netze eine andere Adresse zugewiesen bekommt. Mit Hilfe der NAT-Technik ist dies auf einfache Weise zu realisieren, da hier lediglich die echte Netzadresse (Netzadresse LAN) und die Ersatzadresse (Netzadresse NAT) benötigt werden. Der NAT-Algorithmus sorgt dann dafür, dass ausschließlich für die Kommunikation dieser beiden Netze die Adressen in den Datenpaketen entsprechend ersetzt werden. Man muss also nicht die komplette eigene Netzadressierung anpassen.

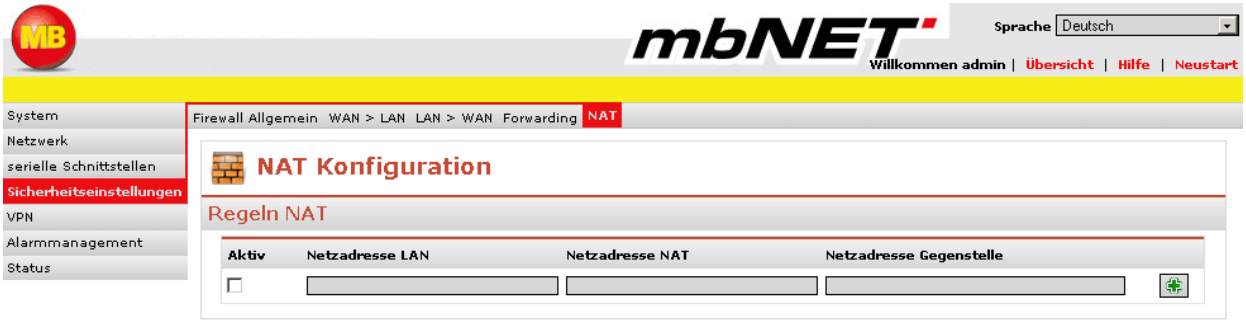


Abbildung 166

Bezeichnung	Beschreibung
Aktiv	Versehen Sie die Checkbox durch Anklicken mit einem Häkchen damit die nachfolgenden Einstellungen nach dem Speichern aktiviert werden.
Netzwerkadresse LAN	Geben Sie hier die reelle Adresse des Netzwerks (z.B. 192.168.0.0/24)ein. **Bitte beachten Sie, dass die CIDR-Schreibweise der IP-Adresse wichtig ist!**
Netzwerkadresse NAT	Geben Sie hier die umgesetzte Adresse ihres Netzwerkes an(z.B. 192.168.1.0/24). **Bitte beachten Sie, dass die CIDR-Schreibweise der IP-Adresse wichtig ist!**
Netzwerkadresse Gegenstelle	Geben Sie hier die Adresse des Netzwerkes ein, zu dem die umgesetzten Pakete geroutet werden sollen. Falls die Gegenstelle auch eine Adressumsetzung verwendet, muss hier die NAT-Adresse der Gegenstelle stehen.
	Aufnahme der neuen Einstellung und temporäres Abspeichern.

16. VPN - IPSec

16.1 Beschreibung zur Konfiguration einer VPN-IPSec Verbindung mit zwei Routern

- ❑ Nachfolgend eine Beschreibung der Einstellungen einer VPN-Verbindung per IPSec-Protokoll.
- ❑ Ausgehend von der Startseite klicken Sie in der linken Navigationsleiste auf **VPN** und in der oberen Navigationsleiste auf **IPSec**.
- ❑ Zum Anlegen einer IPSec-Verbindung betätigen Sie die Schaltfläche rechts.
- ❑ Folgende Bildschirmmaske erscheint:

Abbildung 167

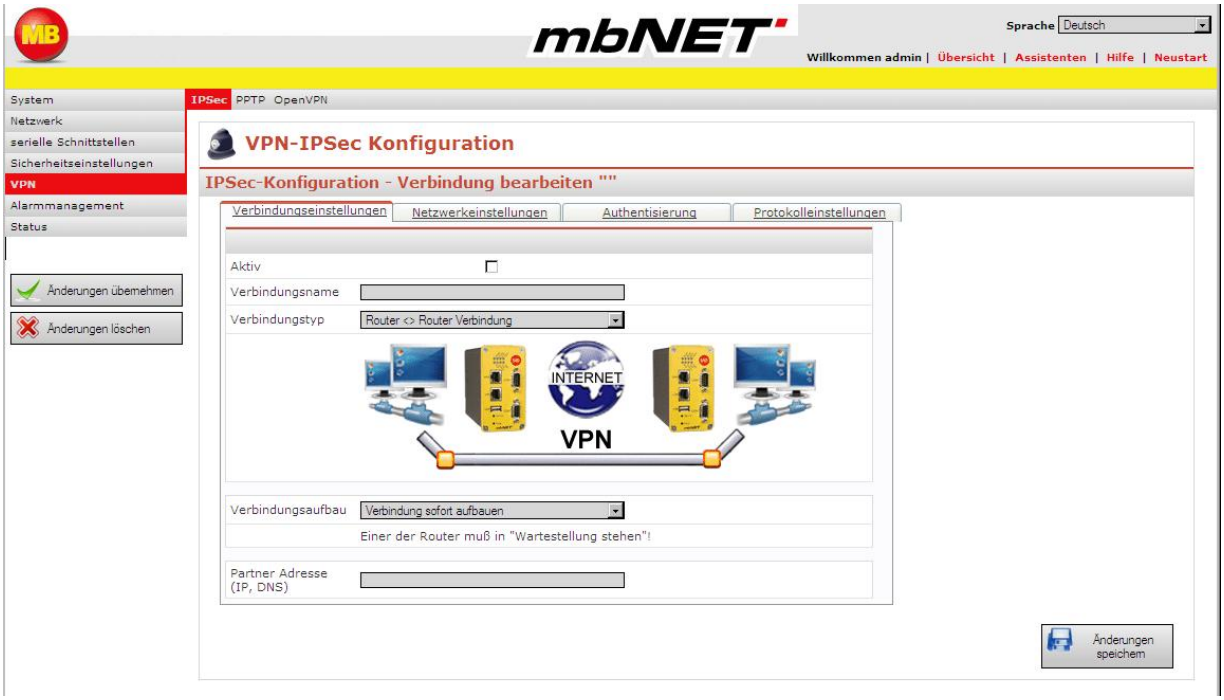


Abbildung 168

16.1.1 Verbindungseinstellungen

Registerkarte	Bezeichnung	Beschreibung
Verbindungseinstellungen	**Aktiv**	Klicken Sie auf die Checkbox um die VPN-Verbindung zu aktivieren.
	Verbindungsname	Tragen Sie in das Eingabefeld einen Namen für die Verbindung ein.
	Verbindungstyp	Wählen Sie über das Auswahlfeld den Verbindungstyp **Router <> Router Verbindung** oder **Client <> Router Verbindung**
	Verbindungsaufbau **(nur bei Router-Router-Verbindung)**	Bitte beachten Sie, dass zur Kommunikation mit einem anderen Router dieser für den Zugang ins Internet und auf Anfragen von Clients entsprechend konfiguriert sein muss. Bei einer ***Router zu Router-Verbindung*** ist unter folgenden Möglichkeiten des Verbindungsaufbaues auszuwählen: **Verbindung sofort aufbauen:** Nach einem Neustart bzw. Bootvorgang wird eine Verbindung aufgebaut. **Verbindung bei Datenverkehr aufbauen** Die Verbindung zum Router bzw. gegenüberliegenden Netzwerk erfolgt bei Anfragen aus dem lokalen Netzwerk. **Warten auf eingehende Verbindung** Der Router der sich in Wartestellung befindet ist der sog. VPN-Server. Er wartet auf eingehende Verbindungen.
	Partner Adresse (IP, DNS) **(nur bei Router-Router Verbindung)**	Beim Router der für die ausgehenden Verbindungen zuständig ist, muss die entsprechende Partneradresse angegeben werden. Dies kann eine IP-Adresse oder auch der DNS-Name sein unter dem der gegenüberliegende Router erreichbar ist.

16.1.2 Netzwerkeinstellungen

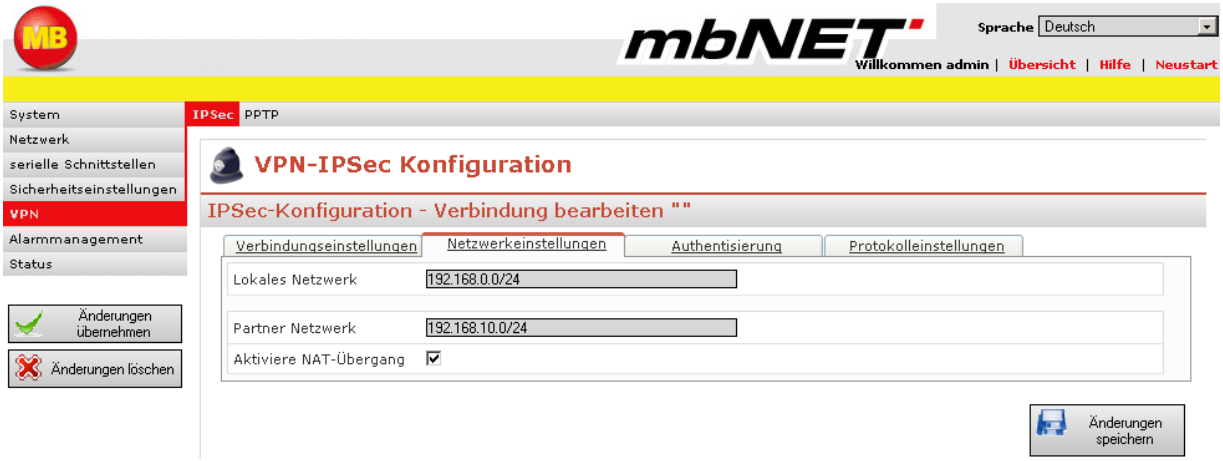


Abbildung 169

16.1.3 Authentisierung

Registerkarte	Bezeichnung	Beschreibung
Netzwerkeinstel-lungen	**Lokales Netzwerk**	Geben Sie hier den Adressbereich des lokalen Netzwerkes in der CIDR-Schreibweise ein. z.B. 192.168.0.0/24
	Partner Netzwerk (nur bei Router-Router-Verbindung)	Geben Sie hier den Adressbereich des lokalen Netzwerkes in der CIDR-Schreibweise ein. z.B. 192.168.10.0/24 ein
	Aktivier NAT-Übergang (nur bei Router-Router-Verbindung)	Diese Einstellung wird benötigt, wenn die VPN-Verbindung über das Internet aufgebaut wird und zwischen dem LAN und dem WAN „genattet“ wird (NAT: Network Address Translation). Diese Einstellung ist in der Regel aktiviert.
	Erlaubtes Netzwerk für den Client: (nur bei Client-Router Ver-bindung)	Stellen Sie hier ein, auf welches Netzwerk der Client zugreifen darf. Die Eingabe erfolgt in der CIDR-Schreibweise.
	Client hat feste IP-Adresse oder Namen (nur bei Client-Router Ver-bindung)	Falls der Client eine feste statische Adresse be-sitzt, dann ist die Adresse im nachfolgenden Ein-gabefeld einzutragen.
	Win2000 / XP Client (L2TP): (nur bei Client-Router Ver-bindung)	Stellen Sie ein ob es sich beim Client um einen PC mit Betriebssystem Windows 2000 oder XP handelt.

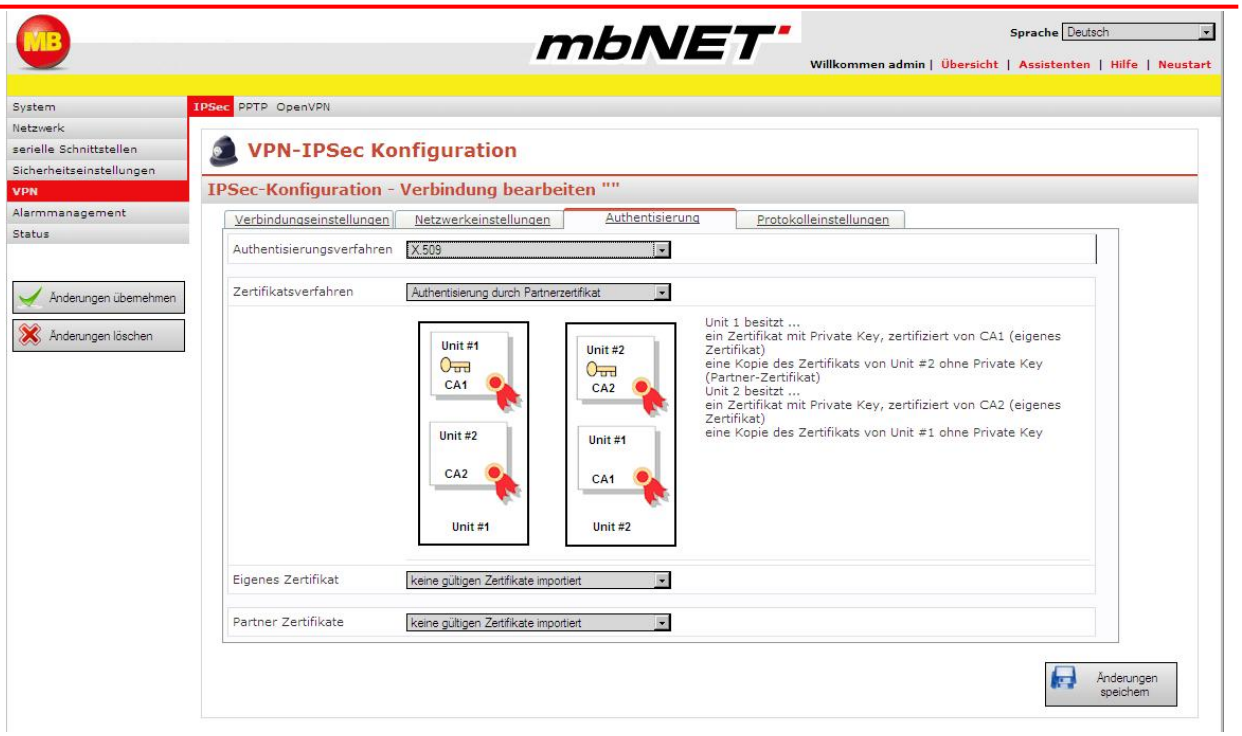
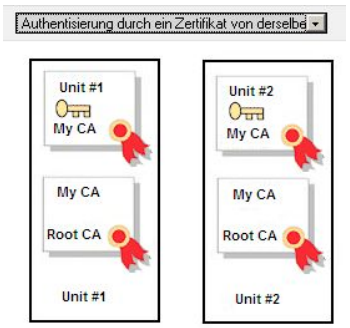
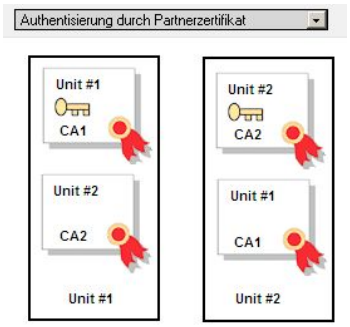


Abbildung 170

Authentisierung(Fortsetzung)

Registerkarte	Beschreibung	
Authentisierung		Wählen Sie über das Auswahlfeld das **Authentisierungsverfahren** aus. **PSK:** Beide Schlüssel müssen vor dem Datenaustausch zwischen Client und Router bekannt sein. Umso länger der Schlüssel ist, umso sicherer ist die Verbindung. Es kann **nur ein** Schlüssel angegeben werden. Auch wenn mehrere PSK-Verbindungen eingetragen werden, gilt für diese nur der Schlüssel der **ERSTEN** Verbindung. **Lokale ID:** Vergeben Sie hier einen Namen für ihren Router. Dieser Name muss dem Partner mitgeteilt werden**.** **Partner ID:** Tragen Sie hier den Namen des Partners ein. **X.509:** **Hierbei können Sie über das Feld unter zwei Zertifikatsverfahren auswählen:** **Authentisierungsverfahren durch eine CA:** Hierzu muss auf dem Router das Stammzertifikat (Unterzeichnende Stelle, kurz CA) und das eigene Zertifikat inklusive Schlüssel (.p12-Datei) importiert sein. (Siehe Kapitel: System – Zertifikate). Die Gegenstelle muss dasselbe Stammzertifikat besitzen und ein von der CA unterzeichnetes Zertifikat inklusive Schlüssel.
		
		

		Authentisierung durch Partnerzertifikate: Hierbei können die Zertifikate von unterschiedlichen CA's unterzeichnet sein. Auf jedem Router muss ein eigenes Zertifikat+Schlüssel (.p12-Datei) importiert sein. Ebenso eine Kopie des jeweiligen Partnerzertifikats, natürlich OHNE Schlüssel (.crt-Datei). **Eigenes Zertifikat:** Wählen Sie das eigene Zertifikat über die Auswahlfläche aus. **Lokale ID:** Diese ID wird normalerweise vom Zertifikat bestimmt. Dieses Feld kann leer gelassen werden. **Partner Zertifikat:** Wählen sie das Zertifikat des Partners aus. **Partner ID:** Diese ID kann nur vom Zertifikat bestimmt werden, wenn man **Authentisierungsverfahren durch Partnerzertifikate** gewählt hat. In diesem Fall kann das Feld leer gelassen werden. Hat man sich jedoch für das **Authentisierungsverfahren durch eine CA** entschieden, so muss man –**nur für den Fall, dass man die Verbindung aufbaut-** die ID des Partners angeben. Diese ID wird beim Erstellen des Zertifikats ausgewählt (siehe Kapitel Zertifikate und Widerrufslisten erstellen mit XCA unter Registerkarte Subjects). Es handelt sich um das sogenannte Subject des Zertifikats und muss in folgender Art und Weise eingetragen werden: */C=land/ST=bundesland/L=stadt/O=firma/OU=abteilung/* *CN=name_zertifikat/E=emailadresse* Wenn bei bei der Erstellung des Zertifikats nicht alle Felder unter der Regsiterkarte **Subject** ausgefüllt hat, so sind die entsprechenden Einträge weg zu lassen (vgl. Kapitel Zertifikate und Widerrufslisten erstellen mit XCA). **Partner Zertifikate:** Nur bei Auswahl **Authentisierung durch Partnerzertifikate**. Auswahl des entsprechenden Zertifikates über das Auswahlfeld.

16.1.4 Protokolleinstellungen

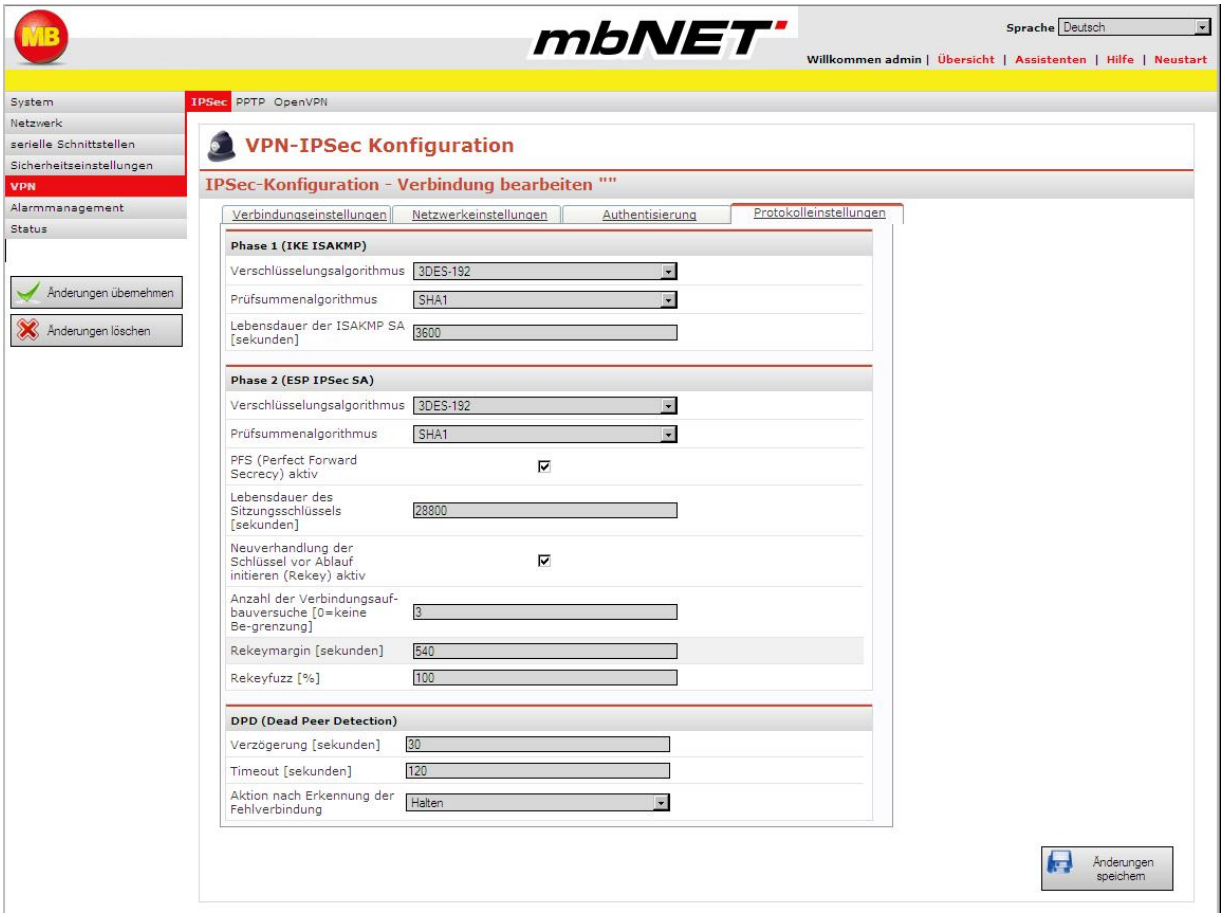


Abbildung 171

Bezeichnung	Beschreibung
Protokollein-stellungen	Wählen Sie hiermit die während der verschiedenen Phasen stattfindenden Ver-schlüsselungsalgorithmen, Prüfsummenbildung usw.
	PFS: Diese Einstellung ist nur für die Router-Router-Verbindung erlaubt. Falls Sie eine Client-Router-Verbindung einrichten möchten, muss PFS deaktiviert werden.

16.1.5 L2TP Server Konfiguration

Für die VPN-IPSec-Kommunikation zwischen dem Industrierouter und einem Windows-Client ist es möglich den L2TP-Server zu verwenden. Hier ist lediglich eine frei wählbare lokale IP-Adresse einzustellen. Aus dem gleichen Netz sollten dann die Adressen für die Clients sein, deren Bereichsanfang und ~ende weiter unten eingestellt werden können. Der L2TP-Server funktioniert dann ähnlich wie ein DHCP-Server und kann die Adressen aus dem eingestellten Bereich an sich einwählende Clients automatisch vergeben.

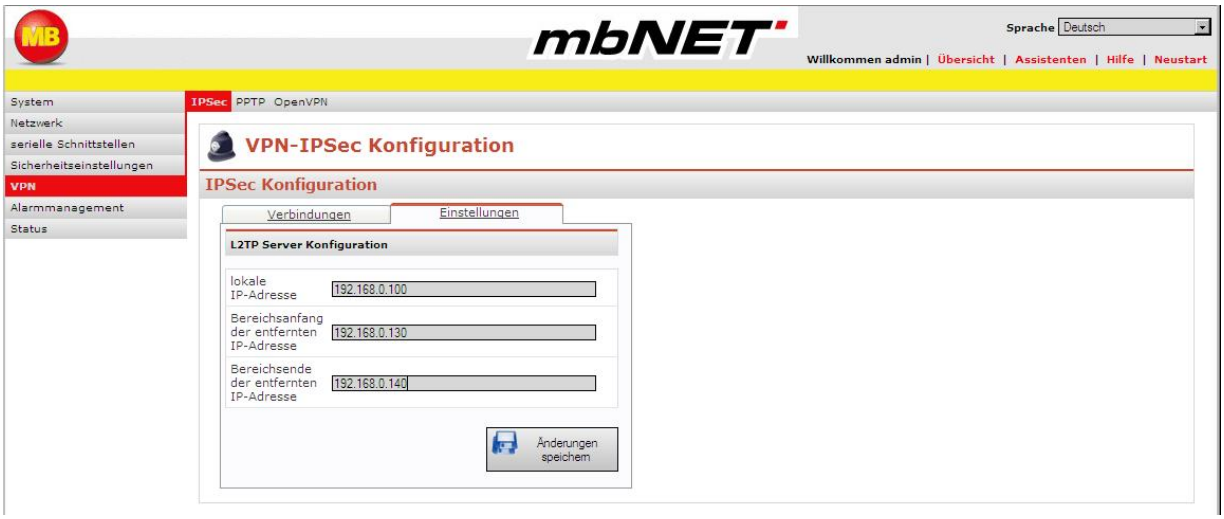


Abbildung 172

Bezeichnung	Beschreibung
Lokale IP-Adresse	Hier ist der Name oder die IP-Adresse einzutragen, die der Server während der Kommunikation mit dem Windows-Client haben soll. Im Beispiel 192.168.0.103
Bereichsanfang der entfernten IP-Adresse **Bereichsende IP-Adresse**	Vergabe der IP-Adressen an Clients. Hier kann der Adressbereich eingestellt werden, aus welchem entfernte Clients ihre IP zugeteilt bekommen. Im Beispiel 192.168.0.130 bis 192.168.0.140

17. VPN - PPTP

17.1 Servereinstellungen

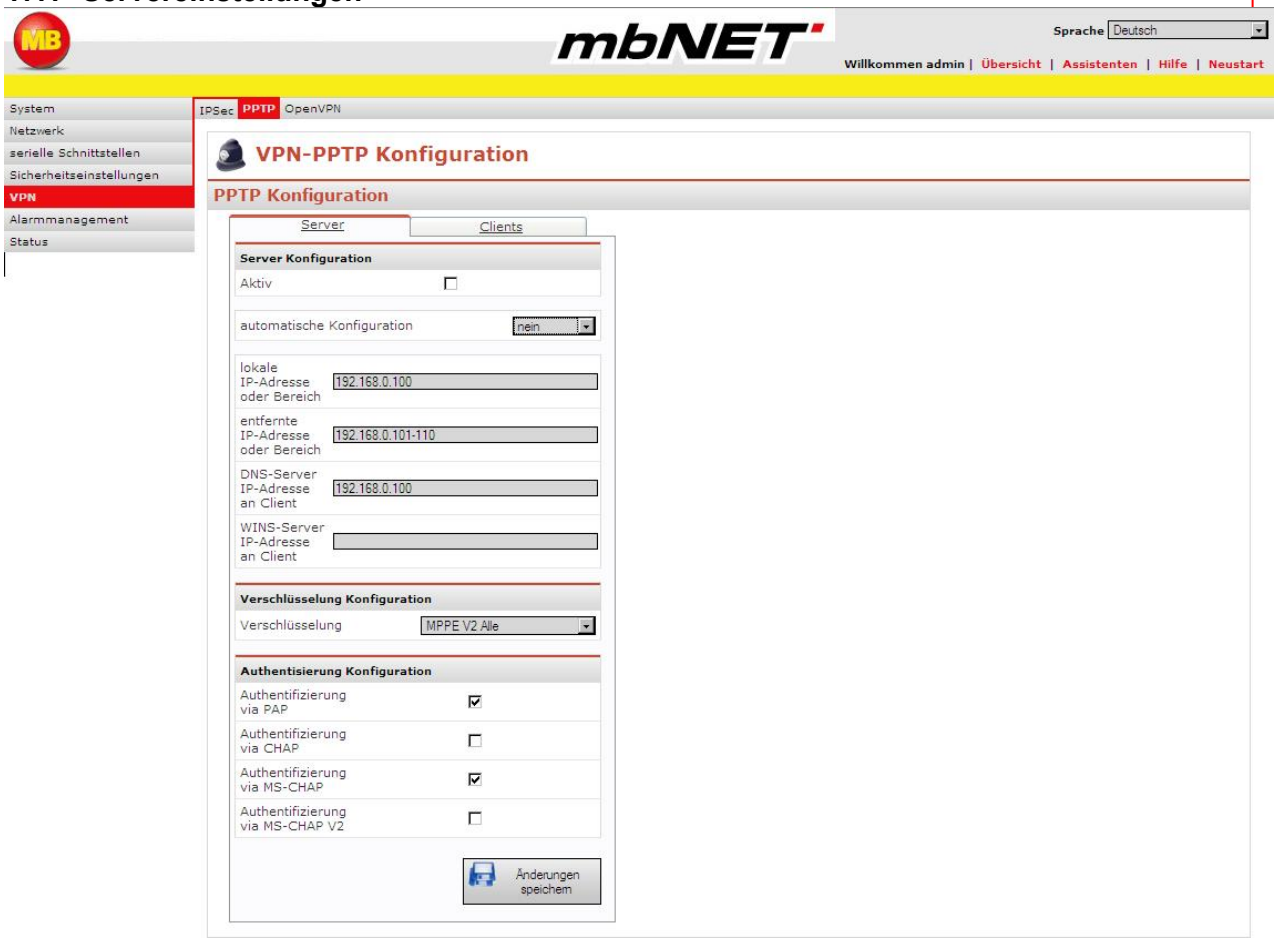


Abbildung 173

Bezeichnung	Beschreibung
Aktiv	Soll der Industrierouter als VPN-Server aktiviert werden, dann ist die Checkbox durch Anklicken mit einem Häkchen versehen.
Automatische Konfiguration	Wenn Sie hier „ja“ auswählen, dann wird die lokale Adresse des mbNET verwendet. Sollten Sie „Nein“ ausgewählt haben, dann beachten Sie folgendes.
Lokale IP Adresse oder Bereich **Entfernte IP Adresse oder Bereich**	Für den Aufbau eines Übertragungskanals ist eine lokale und entfernte Adresse (Anfangs- und Endpunkt des Tunnels) notwendig. Sie haben hier die Möglichkeit entweder eine einzelne IP-Adresse, oder einen ganzen Bereich einzugeben. Bei der Angabe des entfernten Bereichs bestimmt dieser die maximale Anzahl der sich gleichzeitig einwählenden Clients. **Beispiel:** lokale IP-Adresse: 192.168.0.104 Entfernte IP-Adresse: 192.168.0.160 Der VPN-Server ist unter der IP-Adresse 192.168.0.104 erreichbar. Es kann sich nur ein einzelner Client, dem die IP-Adresse 192.168.0.160 (vom Server) zugewiesen wird, am Server anmelden. Beispiel: Lokale IP-Adresse: 192.168.0.104 Entfernte IP-Adresse: 192.168.0.160-170 Den angeschlossenen Clients (max. 10), die sich gleichzeitig einwählen dürfen, werden vom Server 192.168.0.104 die IP-Adressen 192.168.0.160 bis 192.168.0.170 zugewiesen.

VPN - PPTP (Fortsetzung)

Bezeichnung	Beschreibung
DNS-Server IP-Adresse an den Client	Geben Sie hier die DNS-Server-Adresse ein, die einem auf dem Router eingewählten Client zugeordnet wird, um Rechnernamen in IP-Adressen und umgekehrt aufzulösen.
WINS IP-Addresse dem Client zugeordnet.	Tragen Sie hier die WINS-Server-Adresse für die NetBIOS-Namensauflösung ein, die einem, auf dem Router eingewählten, Client zugeordnet wird.
Verschlüsselung	Wählen Sie hier die entsprechende Verschlüsselungsart über das Auswahlfeld: Keine: Keine Verschlüsselung MPPE V2 40:40-BitVerschlüsselung MPPEV2 128: 128-Bit-Verschlüsselung MPPEV2 Alle: Alle Verschlüsselungen
Authentifizierung via PAP	Wählen Sie die Art der Authentifizierung Client schickt dabei dem Host Benutzername / Passwort-Kombination so lange, bis der Host die Authentifizierung des Clients annimmt oder ablehnt.
Authentifizierung via CHAP	Wählen Sie die Art der Authentifizierung Diese Authentizifierung wird vom Host gesteuert. Hat sich ein Client eingewählt, dann wird er vom Host zur Authentifizierung aufgefordert. Die Kombination aus Benutzername und Passwort wird dann vom Client per MD5 verschlüsselt übertragen. Stimmen die gesendeten Benutzerdaten mit denen des Hosts überein, dann wird die Authentifizierung akzeptiert. Wenn nicht, wird sie abgelehnt. Wenn die Authentifizierung akzeptiert wird, werden während der Verbindung dauernd die Benutzerdaten periodisch überprüft.
Authentifizierung via MS-CHAP	Von Microsoft eigenes entwickeltes Authentifizierungsprotokoll.
Authentifizierung via MS-CHAP V2	Von Microsoft eigenes entwickeltes Authentifizierungsprotokoll.

17.2 Clienteinstellung

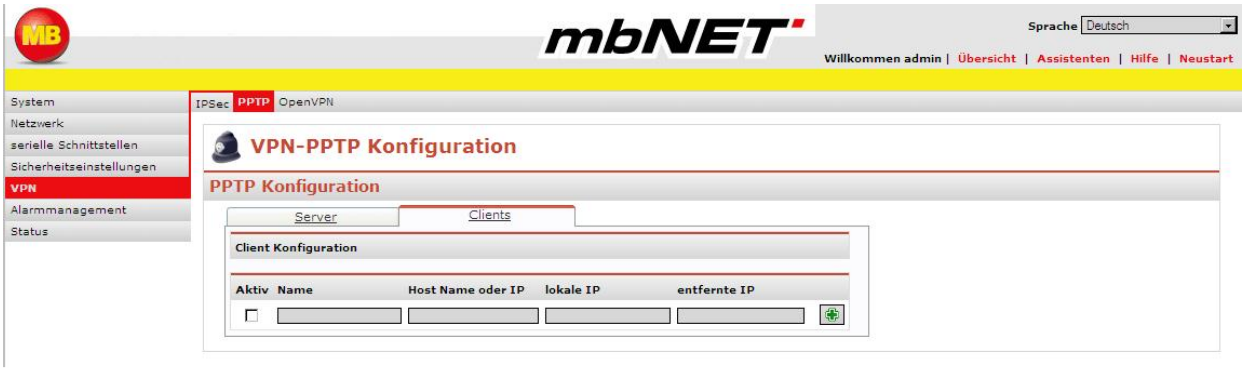


Abbildung 174

Bezeichnung	Beschreibung
Aktiv	Soll der Industrierouter als VPN-Client aktiviert werden, dann ist die Checkbox durch Anklicken mit einem Häkchen versehen.
Name	Tragen Sie hier einen Namen für den Client ein.
Host Name oder IP	Tragen Sie hier den Namen oder die IP-Adresse ein, unter der der Client den Server erreicht. Beispiel 123456789@mbNET.mymbnet.biz oder 80.187.33.55
Lokale IP	**Diese Eingabe ist optional.** Wenn der Server nicht so konfiguriert ist, dass er dem Client eine IP-Adresse zuteilt, dann kann der Client hiermit diese eingetragene IP-Adresse verlangen. In der Regel werden die Einstellungen am VPN-Server durchgeführt. Die Einstellmöglichkeit dient hier der Kompatibilität mit anderen Routern.
Entfernte IP	Tragen Sie hier die Netzadresse des Servers in CIDR-Schreibweise ein (Bsp. 192.168.0.0/24) um eine Route in das Servernetz zu haben.

18. VPN - OpenVPN

18.1 Grundsätzliches zu OpenVPN

- OpenVPN arbeitet grundsätzlich mit zwei Tunnel-IP Adressen. D.h. jede Verbindung hat zwei IP-Adressen über die der Datenverkehr abgewickelt wird.
- abhängig von der Authentifizierungsmethode arbeitet OpenVPN entweder im Punkt-zu-Punkt-Verfahren (bei Statischem Schlüssel oder keiner Authentifizierung) oder im Server/Client-Modus (bei X.509 Zertifikate)
- OpenVPN kann drei verschiedene Authentifizierungsmethoden:
  - **keine** (es ist kein Zertifikat oder Schlüssel notwendig. Dient hauptsächlich zum Testen der Verbindung. Die Tunneldaten werden auch **NICHT** verschlüsselt.)
  - **statischer Schlüssel**. Für die Verbindung wird ein 1024Bit Schlüssel generiert, den jeder Partner benötigt. Ähnlich dem Passwort.
  - **Zertifikate, X.509**. Bei Zertifikaten werden noch folgende Varianten unterschieden:
    - Jeder Teilnehmer benötigt dasselbe RootCA und ein von RootCA unterschriebenes eigenes Zertifikat
    - Wie 1. jedoch noch mit zusätzlicher Benutzer und Passwortabfrage
    - Wie 2. jedoch ohne eigenes Zertifikat. D.h. die Teilnehmer benötigen nur ein RootCA und Benutzer/Passwort.
- OpenVPN kann einen http-Proxyserver als ausgehende Verbindung benutzen. Wichtig bei der Integration in bestehende Firmennetzwerke mit Internetanschluss

- Die Einstellung des Übertragungsprotokolls (UDP oder TCP) ist bei OpenVPN frei einstellbar. Ebenso die dafür zu verwendeten Portnummern.

- ❑ Nachfolgend die Beschreibung der Einstellungen verschiedener Möglichkeiten von OpenVPN-Verbindung

- ❑ Ausgehend von der Startseite klicken Sie in der linken Navigationsleiste auf **VPN** und in der oberen Navigationsleiste auf **OpenVPN**.

- ❑ Zum Anlegen einer OpenVPN-Verbindung betätigen Sie die Schaltfläche rechts.

Abbildung 175

18.2 Verbindungsszenarien

18.2.1 Client – Router

- **Mit dem Verbindungsassistent** können Sie ihre Verbindungen schnell und einfach konfigurieren. Klicken Sie dazu auf der Weboberfläche rechts oben auf den Link „Assistenten“. Wenn Sie die Funktion des automatischen Öffnens des Assistenten deaktiviert haben, dann klicken Sie auf den Start-Knopf des Assistenten für VPN-Verbindungen.

  Bitte beachten Sie, dass Sie erst das Menü unter dem Startknopf des VPN-Assistenten auf „OpenVPN“ umstellen. Danach müssen Sie auf „Änderungen speichern“ und „Änderungen übernehmen“ klicken, damit Sie eine Verbindung mit OpenVPN konfigurieren können

Abbildung 176

- Wählen Sie die Option „Verbindung zwischen einem Client Computer und dem mbNET“

- Danach wählen Sie bitte den statischen Schlüssel aus. Sollten Sie selbst noch keinen erstellt haben, dann können Sie auch den vom mbNET selbst erstellten Schlüssel benutzen. Klicken Sie anschließend auf „Weiter“

- Nach einem Klick auf „Weiter“ ist die Konfiguration der Verbindung abgeschlossen. Klicken Sie auf „Fertigstellen“ um ihre Einstellungen zu übernehmen. Um eine Verbindung aufbauen zu können, müssen Sie OpenVPN auf ihrem Computer installiert haben. Näheres dazu finden Sie bei Kapitel 18.2.1.3 „OpenVPN Windowsclient konfigurieren“.

Abbildung 177

.

Abbildung 178

Registerkarte	Bezeichnung	Beschreibung
Verbindungsein-stellungen	**Aktiv**	Klicken Sie auf die Checkbox um die OpenVPN-Verbindung zu aktivieren.
	Verbindungsname	Tragen Sie in das Eingabefeld einen Namen für die Verbindung ein.
	Verbindungstyp	Wählen Sie über das Auswahlfeld den Verbindungstyp **Client <> Router Verbindung**

Es kann nur eine „Client zu Netzwerk“ Verbindung erstellt werden. Je nach Authentifizierungsmethode erhält der Client eine IP aus einem festgelegten Bereich oder jeder Teilnehmer gibt seine geforderte Adresse vor.

```
Beispiel:

Client PC                    mbNET
[10.1.0.6]  VPN - TUNNEL     [10.1.0.5] <> ROUTING <> LAN [192.168.0.100]
```

18.2.1.1 Keine Authentisierung oder statischer Schlüssel

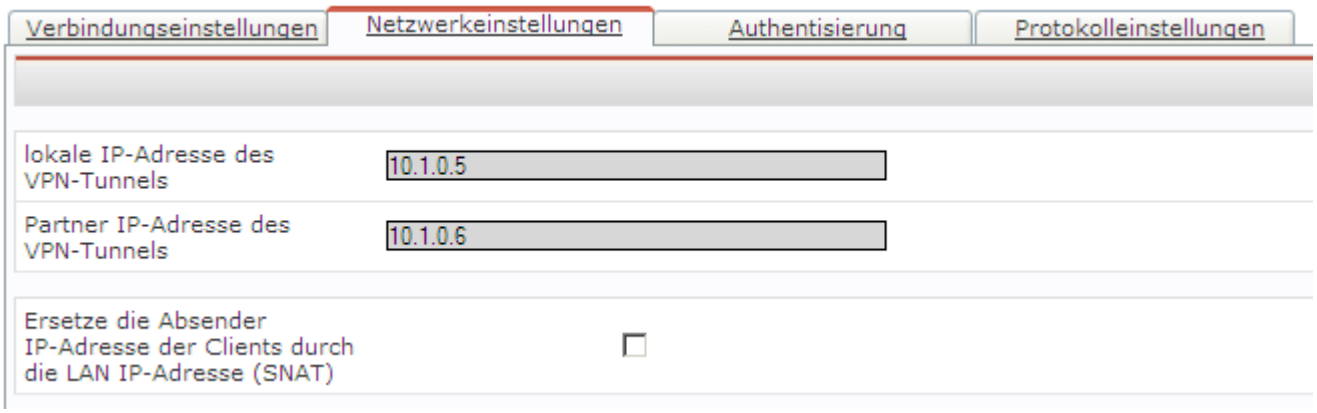


Abbildung 179

Registerkarte	Bezeichnung	Beschreibung
Netzwerk einstellungen	**Lokale IP-Adresse des VPN-Tunnels**	Geben Sie hier die IP Adresse des lokalen VPN Tunnelendpunktes an. z .B. 10.1.0.5
	Partner IP-Adresse des VPN-Tunnels	Geben Sie hier die IP Adresse des Partner VPN Tunnelendpunktes an. z .B. 10.1.0.6
	Ersetze die Absender IP-Adresse der Clients durch die LAN IP-Adresse (SNAT)	Alle Pakete in das LAN-Netzwerk erhalten die Absender IP des mbNET's . Man kann dann zwar im LAN nicht mehr unterscheiden welcher Absender es jetzt ist, aber die Teilnehmer im LAN müssen dann auch das mbNET NICHT als Gateway eingetragen haben.

Bei der Authentifizierung ohne Zertifikate kann pro Verbindungseintrag immer nur ein IP-Kanal vorgegeben werden (IP-Lokal und IP-Partner).

Bei manueller Konfiguration des VPN Clients muss die Einstellung „lokale IP-Adresse des VPN-Tunnels“ und „Partner IP-Adresse des VPN-Tunnels“ auf dem Client entsprechend gedreht werden!

18.2.1.2 Authentisierung mit Zertifikaten

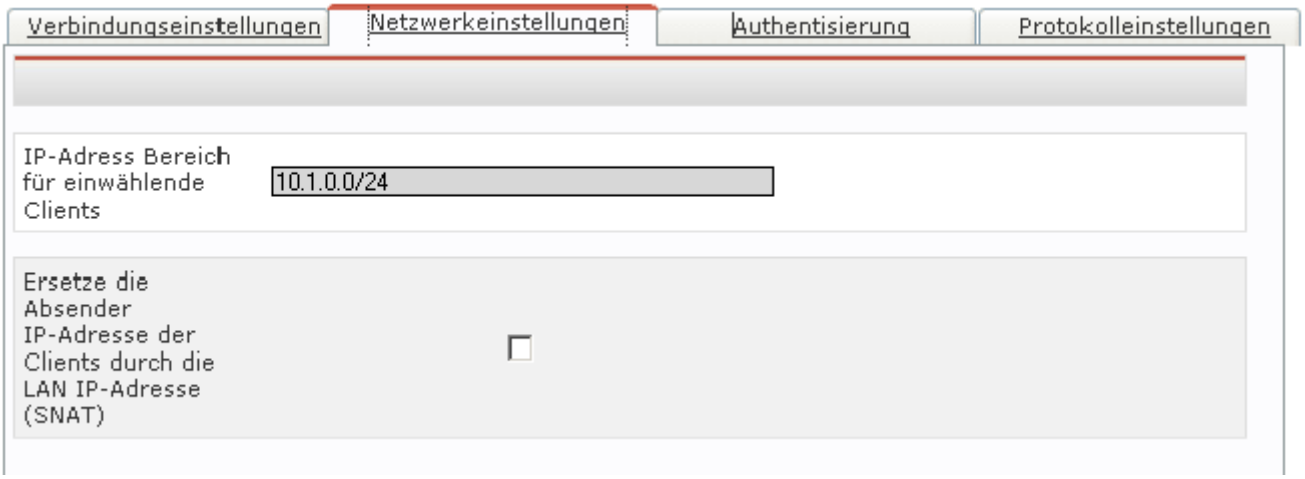


Abbildung 180

Registerkarte	Bezeichnung	Beschreibung

Netzwerk einstellungen	**IP-Adress Bereich für eiwählende Clients**	Bei der Authentifizierung mit Zertifikate können mehrere Clients sich gleichzeitig am Server anmelden und bekommen automatisch eine IP aus dem „IP-Adress-Bereich für einwählende Clients“ zugewiesen. Geben Sie den Adressbereich in der CIDR-Schreibweise ein. z.B. 10.1.0.0/24 (entspricht Netzmaske: 255.255.255.0)
	Ersetze die Absender IP-Adresse der Clients durch die LAN IP-Adresse (SNAT)	Mit der Option „Ersetze die Absender IP-Adresse der Clients durch die LAN IP-Adresse (SNAT)“ kann man erreichen, dass alle Pakete in das LAN-Netzwerk die Absender IP des mbNET’s erhalten. Man kann dann zwar im LAN nicht mehr unterscheiden welcher Absender es jetzt ist, aber die Teilnehmer im LAN müssen dann auch das mbNET NICHT als Gateway eingetragen haben. ACHTUNG, bei mehreren Clients kann das unübersichtlich werden!

Auf der Clientseite muss bzgl. Netzwerkeinstellungen nichts eingestellt werden. In diesem Modus übergibt der Server automatisch alle Informationen an den Client.

18.2.1.3 OpenVPN Windowsclient konfigurieren

Um den OpenVPN Windowsclient nutzen zu können, muss dieser vorher auf dem Computer installiert werden. Die Installationsroutine kann unter der Adresse http://openvpn.net/index.php/open-source/downloads.html heruntergeladen werden.
Die entsprechende Client-Einstellung, kann über den „Download“ Link vom mbNET heruntergeladen werden (Siehe Pfeil). Speichern Sie diese Datei im „config“-Ordner von OpenVPN ab.

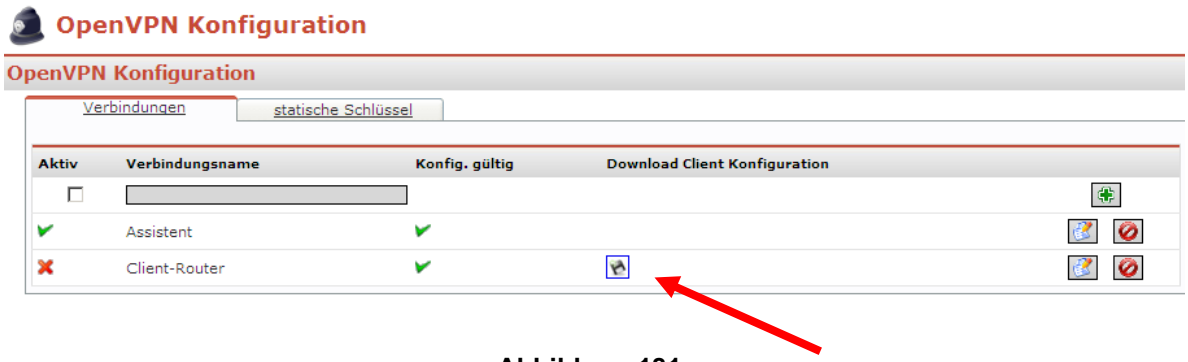


Abbildung 181

Bei manueller Konfiguration des VPN Clients muss die Einstellung „lokale IP-Adresse des VPN-Tunnels“ und „Partner IP-Adresse des VPN-Tunnels“ auf dem Client entsprechend gedreht werden!

Die heruntergeladene Datei entspricht den Einstellungen für OpenVPN für Windows. Öffnen Sie die Einstellungs-Datei mit einem Texteditor um die weiteren Einstellungen vorzunehmen:

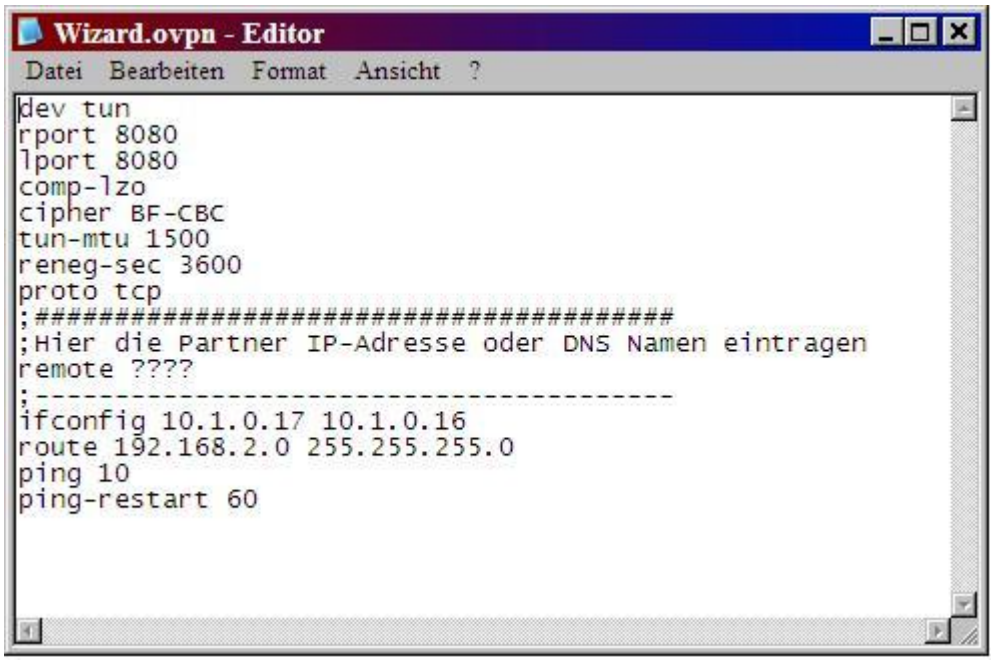


Abbildung 182

18.2.1.3.1 Keine Authentifizierung

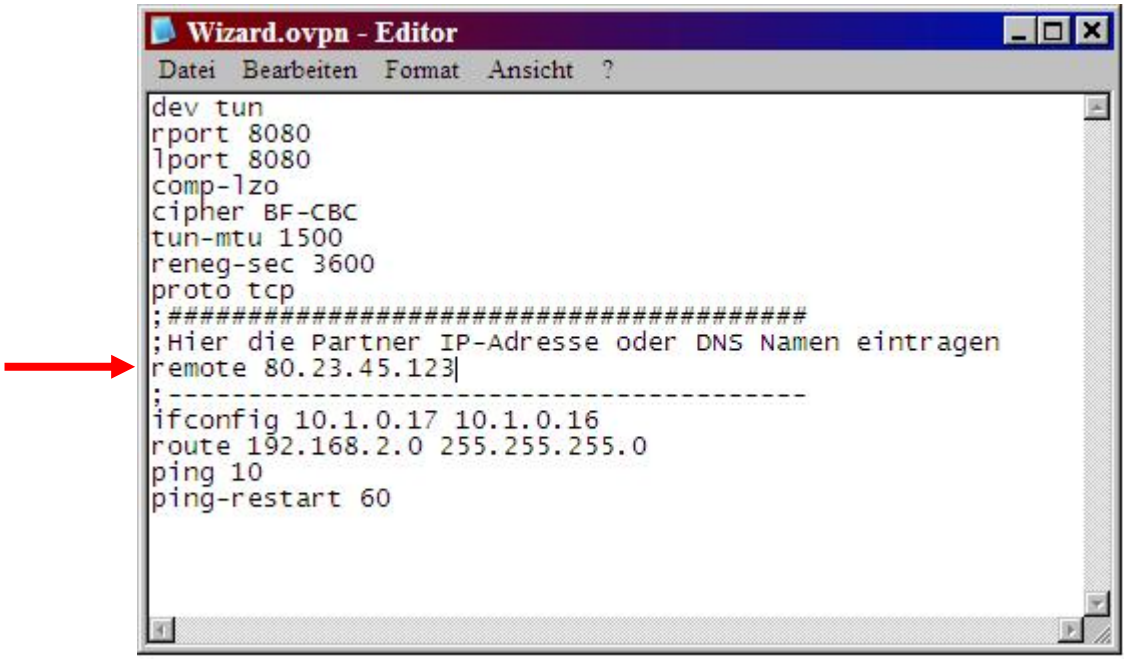


Abbildung 183

Um nun eine OpenVPN-Verbindung ohne Verschlüsselung zu ihrem mbNET aufbauen zu können, müssen Sie nun noch nach „`remote`" die „`????`" löschen. Nun tragen Sie die öffentliche, vom Internet zugänglich IP-Adresse des mbNETs ein, oder nutzen den DynDNS Dienst von MB Connect Line. Dann müssen Sie hier den Namen eingeben, der unter **Netzwerk-DynDNS** angegeben ist.
(Bsp. `remote 0123456789.mbNET.mymbnet.biz`)

18.2.1.3.2 Authentifizierung eines Windowsclient mit statischem Schlüssel

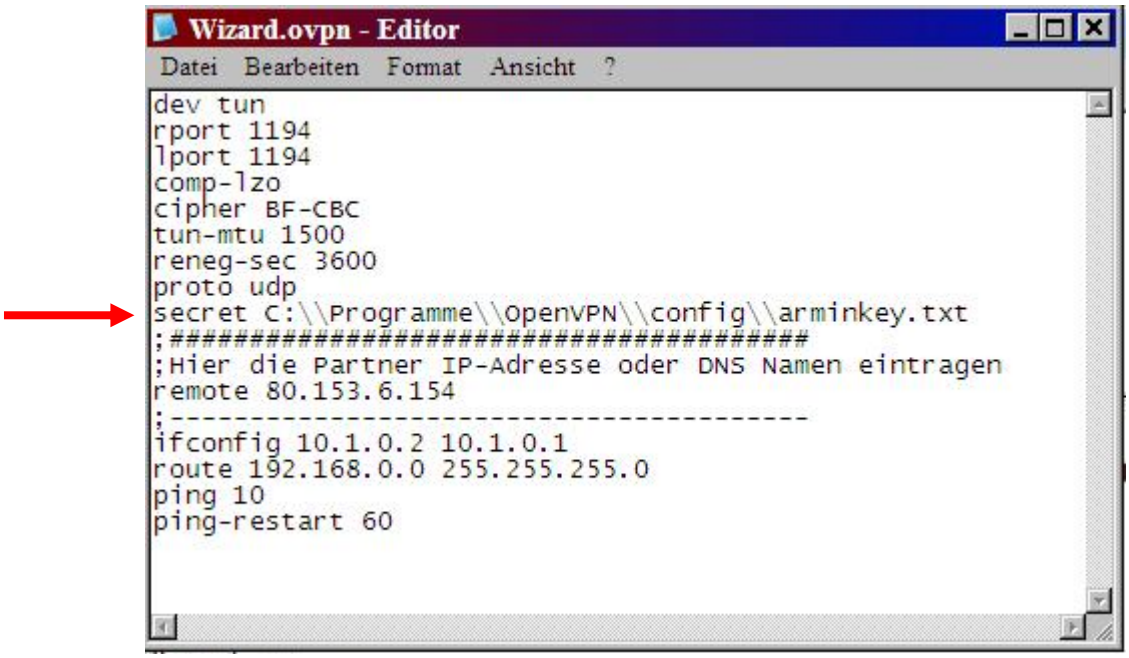


Abbildung 184

Falls Sie sich für die Methode mit dem statischen Schlüssel entschieden haben, dann müssen Sie zusätzlich zur IP-Adresse noch einen Secret-Eintrag vornehmen (Siehe Pfeil). Hierbei ist zu beachten, dass Sie in der Pfadangabe immer **2 Backslashes** verwenden müssen.

Authentifizierung eines Windowsclient mit Zertifikaten

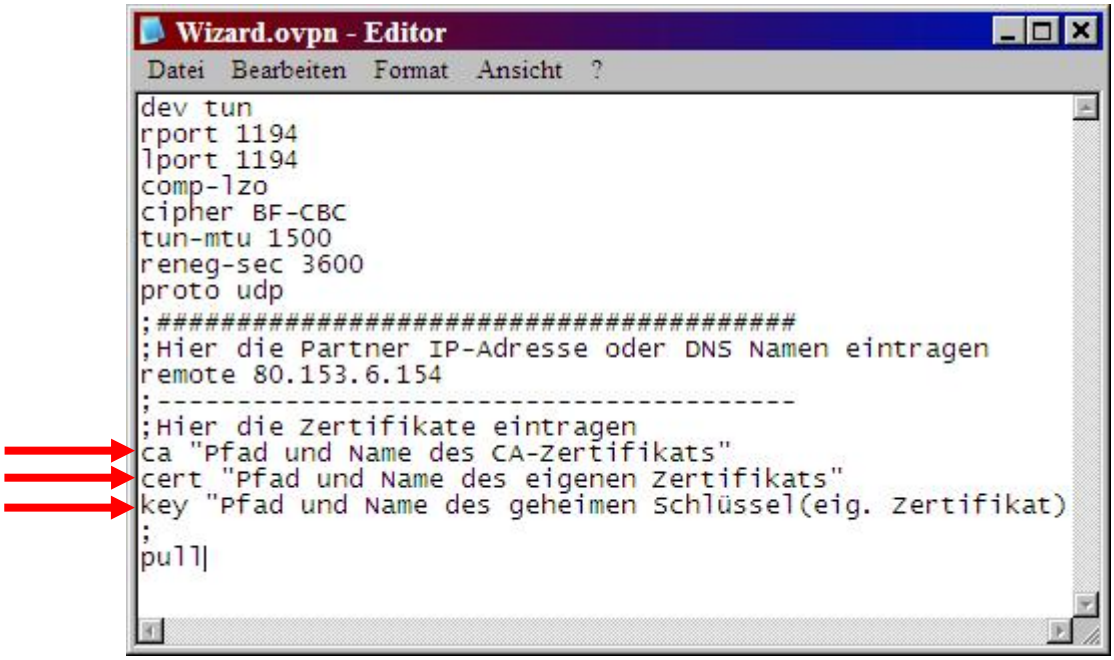


Abbildung 185

ÄnÄndern Sie die markierten Optionen nach ihren Gegebenheiten ab. Hierbei ist zu beachten, dass Sie in der Pfadangabe immer **2 Backslashes** verwenden müssen und Sie benötigen für die Direktive „key“ den Schlüssel ihres eigenen Zertifikats!

18.2.1.3.3 Starten der OpenVPN-Verbindung

Nach dem Abschluss der Konfiguration können Sie einen Rechtsklick auf die .ovpn-Datei ausführen, oder wie unten angezeigt die Verbindung über das über die grafische Oberfläche in der Leiste starten.

Abbildung 186

18.2.2 Router-Router

- **Mit dem Verbindungsassistent:** Klicken Sie auf der Weboberfläche rechts oben auf den Link „Assistenten“ klicken Sie auf den Start-Knopf des Assistenten für VPN-Verbindungen und klicken auf „Weiter“.
- Wählen Sie „Verbinden von 2 Netzwerken“ aus(Abb.158)
- Im folgenden Fenster wählen Sie den VPN-Server aus und klicken wieder auf „Weiter“.
- Anschließend müssen Sie die lokale Netz-adresse und die Subnetzmaske des VPN-Clients angeben (Abb. 159)
- Stellen Sie den Schlüssel ihrer Wahl im fol-genden Fenster ein, oder benutzen Sie den vom mbNET generierten Schlüssel.
- Drücken Sie zum Abschluss der Konfiguration auf „Fertigstellen“ um ihre Einstellungen zu übernehmen. Wiederholen Sie diese Konfigu-ration mit dem VPN-Client. Jedoch müssen Sie anstatt VPN-Server, VPN-Client wählen.

Abbildung 187

Abbildung 188

Abbildung 189

Registerkarte	Bezeichnung	Beschreibung
Verbindungs-einstellungen	**Aktiv**	Klicken Sie auf die Checkbox um die OpenVPN-Verbindung zu aktivieren.
	Verbindungsname	Tragen Sie in das Eingabefeld einen Namen für die Verbindung ein.
	Verbindungsaufbau	Wählen Sie über das Auswahlfeld den Verbindungstyp ,

Hier kann eine „Netzwerk zu Netzwerk“ Verbindung erstellt werden. Je nach Authentifizierungsmethode erhält der Einwählende eine IP aus einem festgelegten Bereich oder jeder Teilnehmer gibt seine geforderte Adresse vor.

```
Beispiel:

LAN                    mbNET Client                    mbNET Server LAN
[192.168.99.100]<>ROUTING<>[10.1.0.2] VPN - TUNNEL [10.1.0.1]<>ROUTING<>[192.168.0.100]
```

Verbindungsaufbau
Warten auf eingehende Verbindung
Verbindung sofort aufbauen
Starten bei aktiver Internetverbindung
Warten auf eingehende Verbindung
Starten wenn Eingang 1 aktiv ist (1-Signal)
Starten wenn Eingang 2 aktiv ist (1-Signal)
Starten wenn Eingang 3 aktiv ist (1-Signal)
Starten wenn Eingang 4 aktiv ist (1-Signal)
Starten wenn die Dialout Taste gedrückt wurde
en"!

Abbildung 190

Wurde für den Verbindungsaufbau « Warten auf eingehende Verbindung » gewählt, so ist dieses mbNET im Server Modus und wird in der weiteren Dokumentation als „Server“ benannt.
Wurde für den Verbindungsaufbau « Verbindung sofort aufbauen » oder « Starten bei aktiver Internetverbindung » gewählt, so ist dieses mbNET im Client Modus und als „Client“ benannt.

18.2.2.1 Server – keine Authentifizierung oder statischer Schlüssel

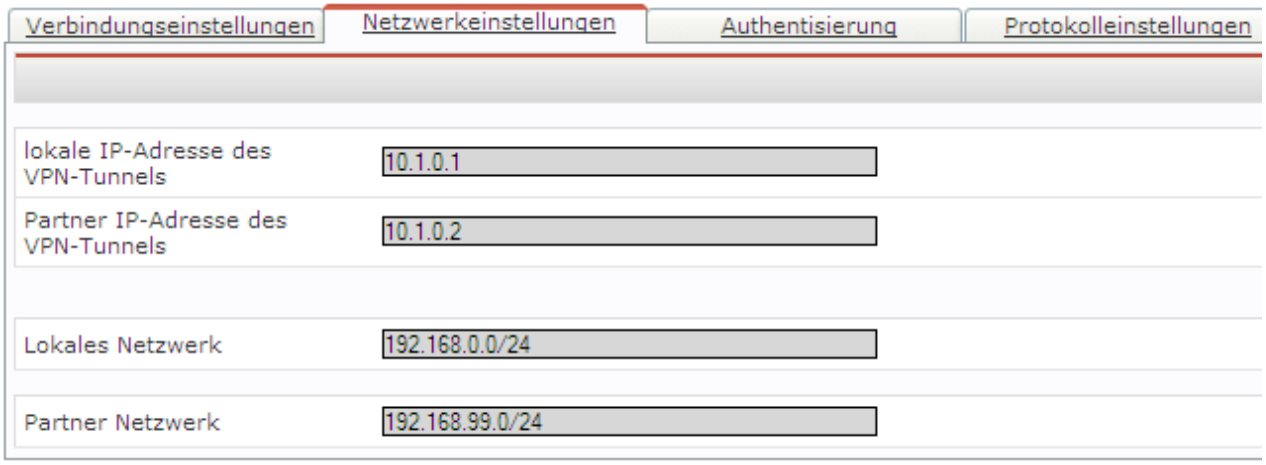


Abbildung 191

Registerkarte	Bezeichnung	Beschreibung
Netzwerk-einstellungen	**lokale IP-Adresse des VPN-Tunnels**	Geben Sie hier die IP Adresse des lokalen VPN Tunnelendpunktes an. z .B. 10.1.0.1
	Partner IP-Adresse des VPN-Tunnels	Geben Sie hier die IP Adresse des Partner VPN Tunnelendpunktes an. z .B. 10.1.0.1
	Lokales Netzwerk	Tragen Sie hier ihre Netzwerkadresse in der CIDR-Schreibweise ein (192.168.0.0/24)
	Partner Netzwerk	Tragen Sie hier die Netzadresse ihres Partners der CIDR-Schreibweise ein (192.168.5.0/24).

Bei der Authentifizierung ohne Zertifikate kann pro Verbindungseintrag immer nur ein IP-Kanal vorgegeben werden (IP-Lokal und IP-Partner).

> Bei manueller Konfiguration des VPN Clients muss die Einstellung „lokale IP-Adresse des VPN-Tunnels“ und „Partner IP-Adresse des VPN-Tunnels“ auf dem Client entsprechend gedreht werden!

18.2.2.2 Server – Authentifizierung mit Zertifikaten

Bei der Authentifizierung mit Zertifikate können mehrere Clients sich gleichzeitig am Server anmelden und bekommen automatisch eine IP aus dem „IP-Adressbereich für einwählende Clients“ zugewiesen
Im Server Modus mit Zertifikaten werden zwei Betriebsarten unterschieden.

18.2.2.2.1 Single Client: nur ein Client kann sich einwählen

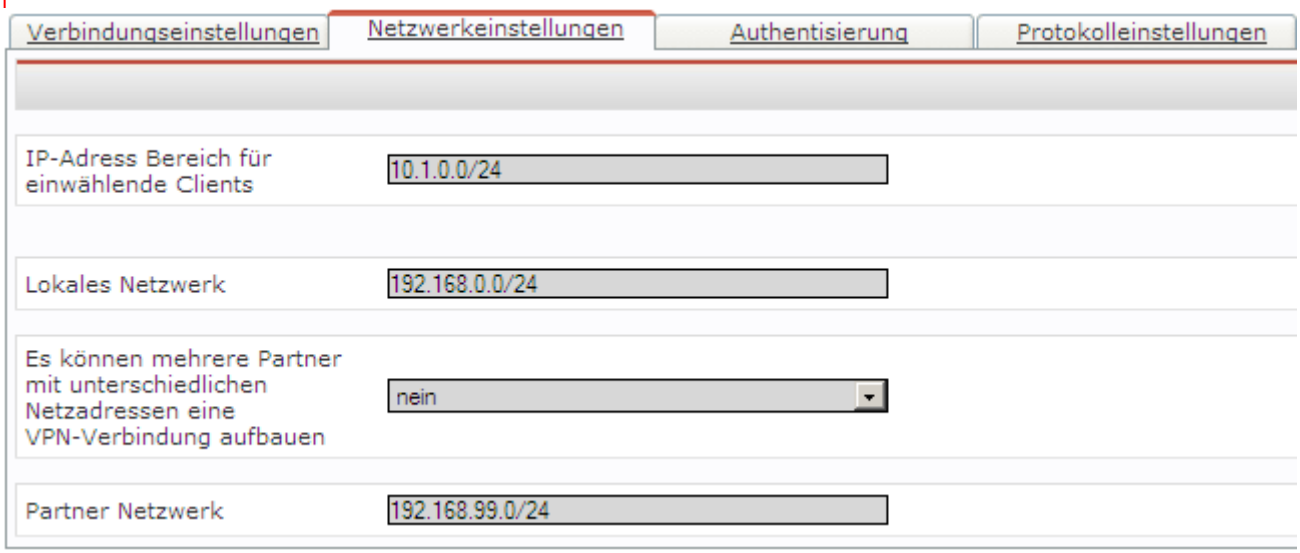


Abbildung 192

Registerkarte	Bezeichnung	Beschreibung
Netzwerkeinstellungen	**IP-Adressbereich für einwählende Clients**	Bei der Authentifizierung mit Zertifikate können mehrere unterschiedliche Clients sich am Server anmelden (nicht gleichzeitig) und bekommen automatisch eine IP aus dem „IP-Adressbereich für einwählende Clients“ zugewiesen. Geben Sie den Adressbereich in der CIDR-Schreibweise ein. Z.B. 10.1.0.1/24
	Lokales Netzwerk	Tragen Sie hier den Adressbereich des lokalen Netzwerkes in der CIDR-Schreibweise ein. z.B. 10.1.0.2/24
	Es können mehrere Partner mit unterschiedlichen Netzadressen eine VPN-Verbindung aufbauen.	Auswahl „nein“ Jeder Client bekommt den Partnernetzwerk- Adressbereich zugewiesen, somit ist eine Einwahl von gleichzeitigen Clients hier nicht sinnvoll.
	Partner Netzwerk	Tragen Sie hier die Netzadresse ihres Partners der CIDR-Schreibweise ein (192.168.99.0/24).

Am Client muss keine Netzwerkeinstellung vorgenommen werden, diese wird vom Server an den Client gesendet.

Es muss das lokale Netzwerk und das Partnernetzwerk angegeben werden. Anhand dieser Einträge erstellt OpenVPN dann die notwendigen Routingeinträge

18.2.2.2.2 Multi Client: mehrere Clients können sich einwählen

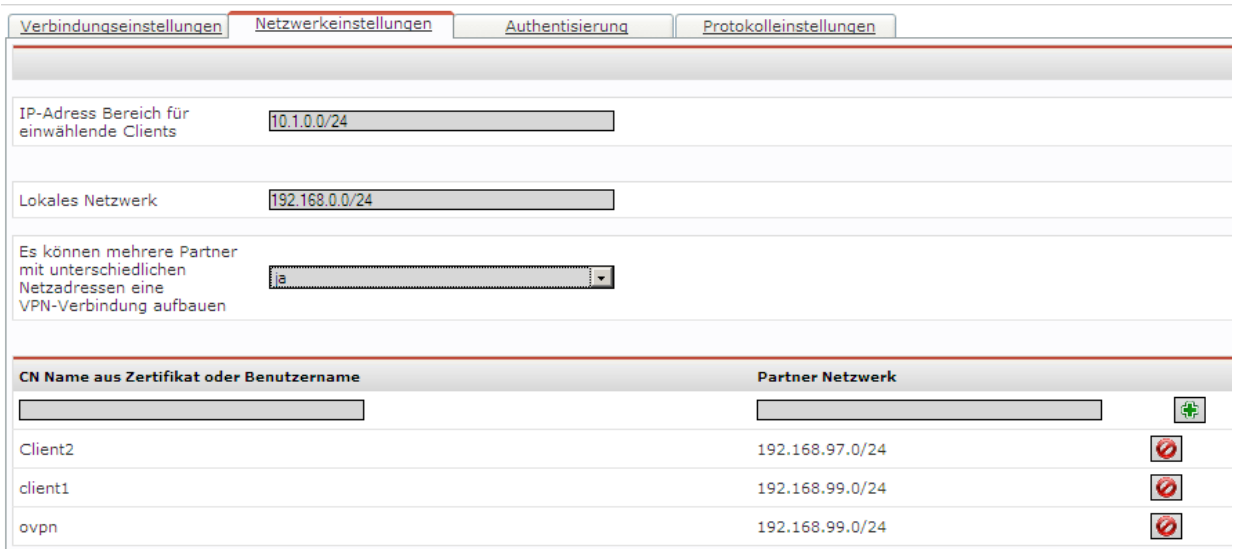


Abbildung 193

Registerkarte	Bezeichnung	Beschreibung
Netzwerk-einstellungen	**IP-Adress Bereich für einwählende Clients**	Bei der Authentifizierung mit Zertifikaten können sich mehrere unterschiedliche Clients gleichzeitig am Server anmelden und bekommen automatisch eine Adresse aus dem „IP-Adress Bereich für einwählende Clients“ zugewiesen. Geben Sie den Adressbereich in der CIDR-Schreibweise ein. Z.B. 10.1.0.1/24
	Lokales Netzwerk	Tragen Sie hier den Adressbereich des lokalen Netzwerkes in der CIDR-Schreibweise ein. z.B. 10.1.0.2/24
	Es können mehrere Partner mit unterschiedlichen Netzadressen eine VPN-Verbindung aufbauen.	Auswahl „Ja“ Bei der Authentifizierung mit Zertifikaten und diesem Betriebsmodus, können mehrere Clients sich gleichzeitig am Server anmelden und bekommen automatisch eine Adresse aus dem „IP-Adressbereich für einwählende Clients“ zugewiesen
	CN aus Zertifikat oder Benutzername	Es muss das lokale Netzwerk (oben) und das Partnernetzwerk angegeben werden. In der unteren Liste wird jedem Client ein Netzwerk zugewiesen. Je nach Einstellung in der Authentifizierung (mit Zertifikatsnamen oder Benutzernamen) kann der CN (Common Name im Zertifikat) oder Benutzername ausschlaggebend sein. OpenVPN erstellt je nach gerade einwählendem Client einen entsprechenden Routingeintrag

Am Client muss keine Netzwerkeinstellung vorgenommen werden, diese wird vom Server an den Client gesendet.

18.2.2.3 Client –Authentifizierung: kein oder statischer Schlüssel

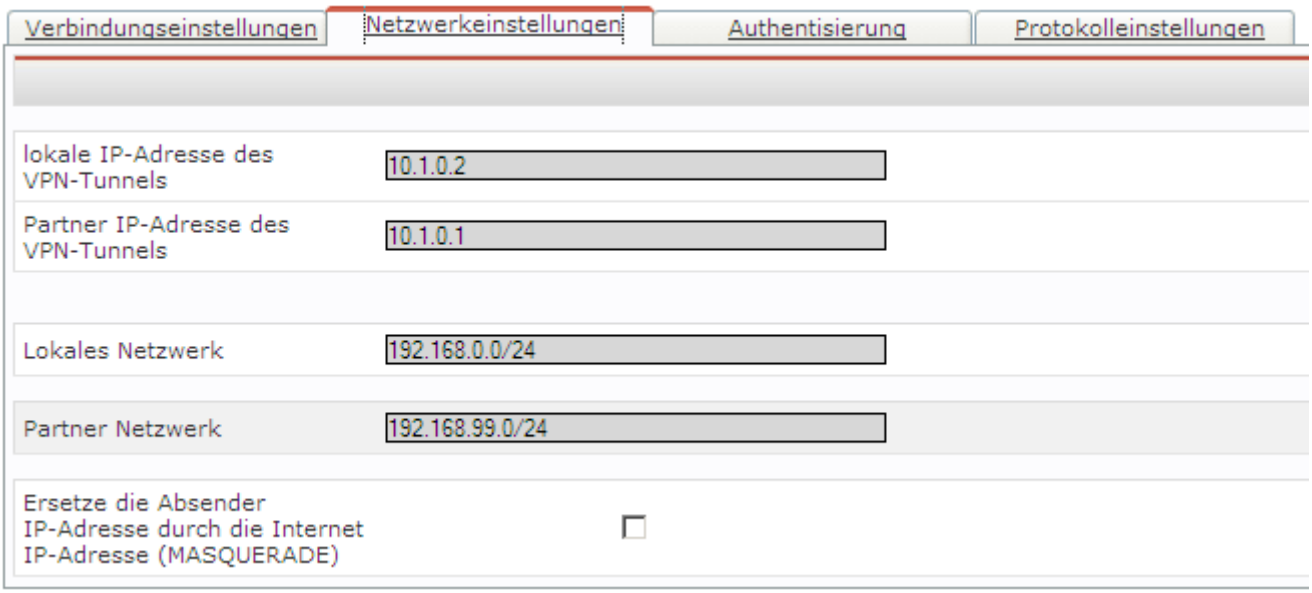


Abbildung 194

Registerkarte	Bezeichnung	Beschreibung
Netzwerkeinstellungen	**lokale IP-Adresse des VPN-Tunnels**	Geben Sie hier die IP Adresse des lokalen VPN Tunnelendpunktes an. z .B. 10.1.0.2
	Partner IP-Adresse des VPN-Tunnels	Geben Sie hier die IP Adresse des Partner VPN Tunnelendpunktes an. z .B. 10.1.0.1
	Lokales Netzwerk	Tragen Sie hier ihre Netzwerkadresse in der CIDR-Schreibweise ein (192.168.0.0/24)
	Partnernetzwerk	Tragen Sie hier die Netzadresse ihres Partners der CIDR-Schreibweise ein (192.168.5.0/24).
	Ersetze die Absender IP-Adresse durch die Internet IP-Adresse (MASQUERADE)	Diese Option wurde für die Kompatibilität mit mdex eingeführt. Wie die Option schon beschreibt wird die Absender IP-Adresse durch die aktuelle Internet-IP-Adresse ersetzt

Bei der Authentifizierung ohne Zertifikate kann pro Verbindungseintrag immer nur ein IP-Kanal vorgegeben werden. IP-Lokal und IP-Partner

Die Einstellung „lokale IP-Adresse des VPN-Tunnels“ und „Partner IP-Adresse des VPN- Tunnels“ vom Server, muss auf dem Client entsprechend gedreht werden!

18.2.2.4 Client – Authentifizierung: mit Zertifikate

Abbildung 195

Registerkarte	Bezeichnung	Beschreibung
Netzwerk-einstellungen	**Ersetze die Absender IP-Adresse durch die Internet IP-Adresse (MASQUERADE)**	Diese Option wurde für die Kompatibilität mit mdex eingeführt. Wie die Option schon beschreibt wird die Absender IP-Adresse durch die aktuelle Internet-IP-Adresse ersetzt

Am Client muss keine Netzwerkeinstellung vorgenommen werden, diese wird vom Server an den Client gesendet.

18.2.3 Authentifizierung

OpenVPN bietet drei grundsätzlich unterschiedliche Authentifizierungsarten an.

- keine (es ist kein Zertifikat oder Schlüssel notwendig. Dient hauptsächlich zum Testen der Verbindung. Die Tunneldaten werden auch NICHT verschlüsselt.)
- statischer Schlüssel. Für die Verbindung wird ein Schlüssel generiert, den jeder Partner benötigt. Ähnlich einem Passwort.
- Zertifikate, X.509. Bei Zertifikaten werden drei Varianten unterschieden:
    - Jeder Teilnehmer benötigt dasselbe RootCA und ein von RootCA unterschriebenes eigenes Zertifikat
    - Wie 1. jedoch noch mit zusätzlicher Benutzer und Passwortabfrage
    - Wie 2. jedoch ohne eigenes Zertifikat. D.h. die Teilnehmer benötigen nur ein RootCA und Benutzer/Passwort.

18.2.3.1 Keine Authentifizierung

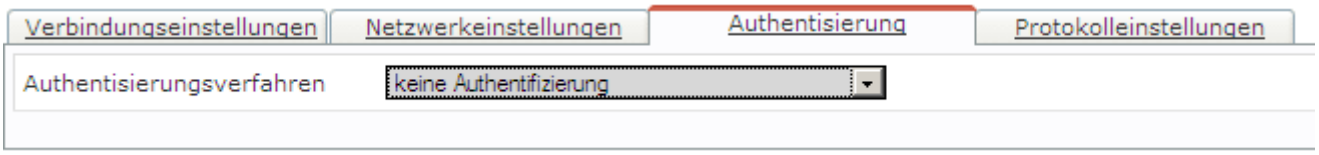


Abbildung 196

Diese Einstellung soll hauptsächlich zu Testzwecken dienen. Man kann hier sehr schnell und einfach die Verbindung zu einem Partner testen. Z.B. ob die richtigen Ports freigeschaltet sind. In diesem Modus werden die Daten UNVERSCHLÜSSELT versendet.

18.2.3.2 Authentifizierung mit statischem Schlüssel

Abbildung 197

Bei der symmetrischen Verschlüsselung erfolgt die Authentifizierung und Ver- bzw. Entschlüsselung der Daten mit ein und demselben Schlüssel (statischer Schlüssel). Der Vorteil der symmetrischen Verschlüsselung ist die Geschwindigkeit. Das Ver- und Entschlüsseln dauert im Gegensatz zur asymmetrischen Verschlüsselung deutlich weniger lang, da der symmetrische Schlüssel schon ab 90Bit als sicher gilt – der asymmetrische dagegen sollte mindestens 1.024 Bit lang sein. Der Nachteil der symmetrischen Verschlüsselung ist der gegenseitige Schlüsselaustausch. Jeder Teilnehmer muss den Schlüssel auf sichere Art und Weise erhalten.
In der obigen Maske kann ein zuvor importierter oder generierter Schlüssel ausgewählt werden.

18.2.3.2.1 Schlüsselmanagement

Sie können einen Schlüssel importieren oder selbst generieren. Alle enthaltenen Schlüssel können als Kopie unter „Download“ heruntergeladen werden.

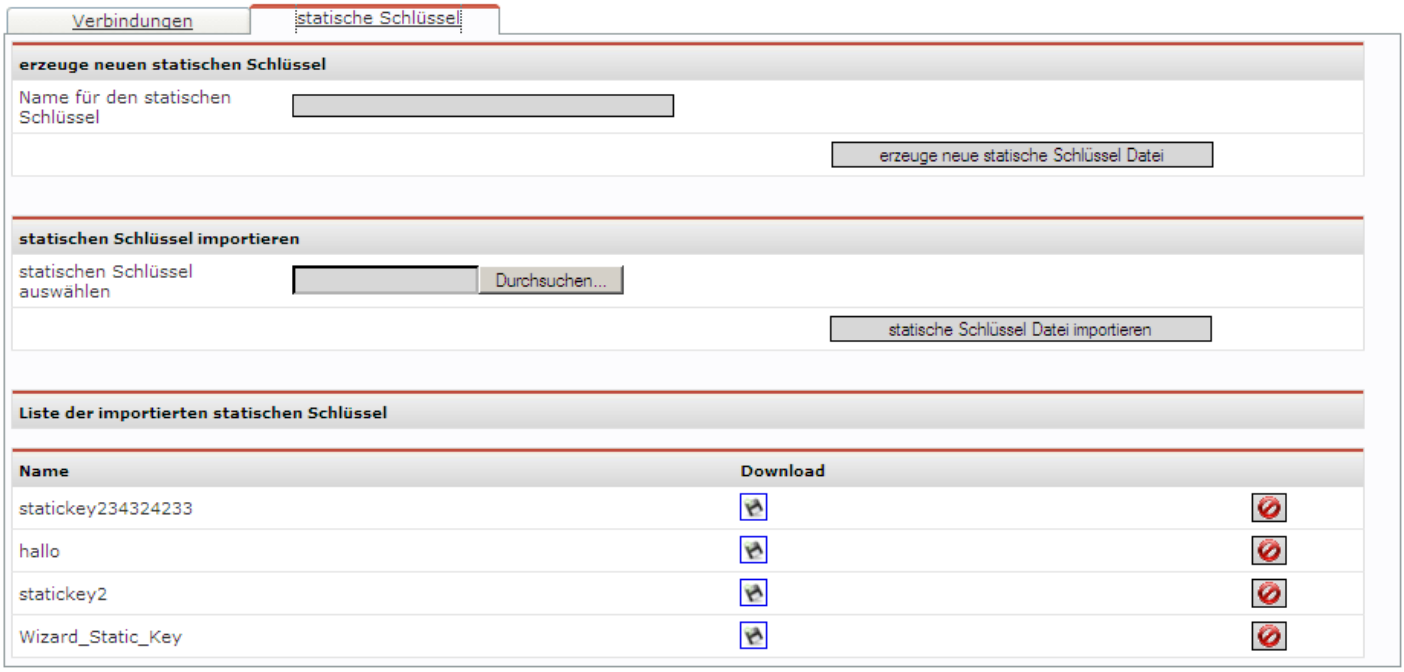


Abbildung 198

Registerkarte	Bezeichnung	Beschreibung
Statische Schlüssel	**Name für den statischen Schlüssel**	Geben Sie hier den Namen des Schlüssels ein, der generiert werden soll.
	Statischen Schlüssel auswählen	Hier kann ein Schlüssel importiert werden, der vorher auf einem anderen System generiert worden ist.

18.2.3.3 Authentisierung mit Zertifikate

Bei der Authentifizierung mit Zertifikaten unterscheidet man drei Varianten:

1. Jeder Teilnehmer benötigt dasselbe RootCA und ein von RootCA unterschriebenes eigenes Zertifikat
2. Wie 1. jedoch noch mit zusätzlicher Benutzer und Passwort abfrage
3. Wie 2. jedoch ohne eigenes Zertifikat. D.h. die Teilnehmer benötigen nur ein RootCA und Benutzer/Passwort.

18.2.3.3.1 Authentifizierung mit CA- und eigenem Zertifikat

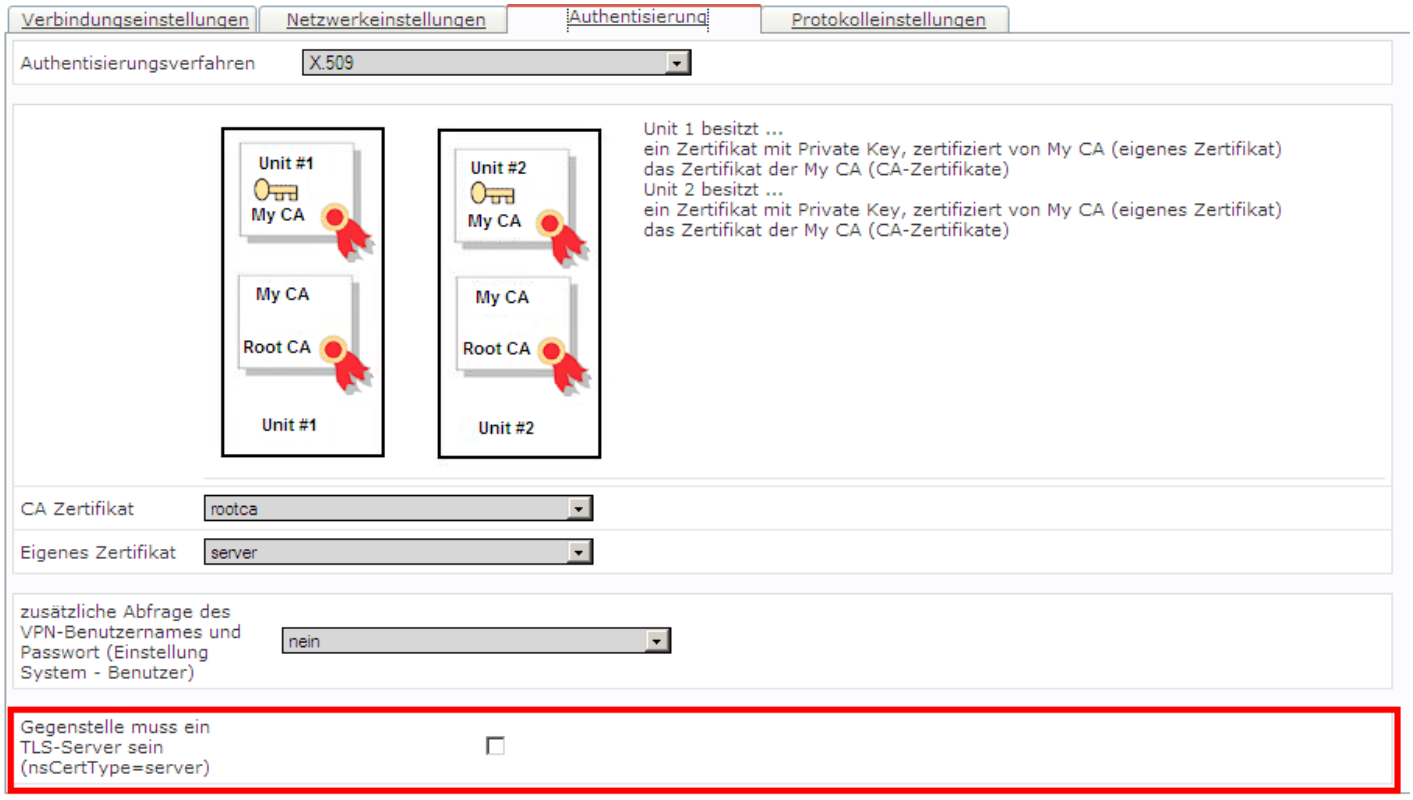


Abbildung 199

Registerkarte	Bezeichnung	Beschreibung
Authentisierung X.509	**CA Zertifikat**	Dies ist das Stammzellenzertifikat(RootCA). Von diesem Zertifikat müssen alle anderen Zertifikate abstammen
	Eigenes Zertifikat	Mit diesem Zertifikat authentifizieren Sie sich gegenüber ihrem VPN-Partner
	Zusätzlich Abfrage des VPN-Benutzernamens und Passwort	Es ist möglich, dass zusätzlich noch Benutzerdaten von einwählenden Client gefordert werden. Bitte beachten Sie hierbei, dass diese Benutzerdaten im VPN-Server unter *System-Benutzer* eingetragen sein müssen
	Benutzerdaten	Tragen Sie hier die Benutzerdaten vom VPN-Server (aus System-Benutzer) ein
	Das eigene Zertifikat nicht für die Authentifizierung benutzen. Nur das CA Zertifikat und die Benutzerdaten verwenden	Mit dieser Option authentifizieren Sie sich nur über das CA-Zertifikat und die Benutzerdaten des VPN-Servers (aus System-Benutzer)
	Gegenstelle muss ein TLS-Server sein	Dies ist eine zusätzliche Sicherheitsoption. Das „Server-Zertifikat“ muss den Zusatz `nsCertType=server` unbedingt eingetragen haben (siehe Kapitel Erstellen von Zertifikaten).

18.2.3.3.2 Authentifizierung mit CA- und eigenem Zertifikat und Benutzer/Passwort

Die Einstellung unterscheidet sich je nach Modus.

18.2.3.3.3 Server

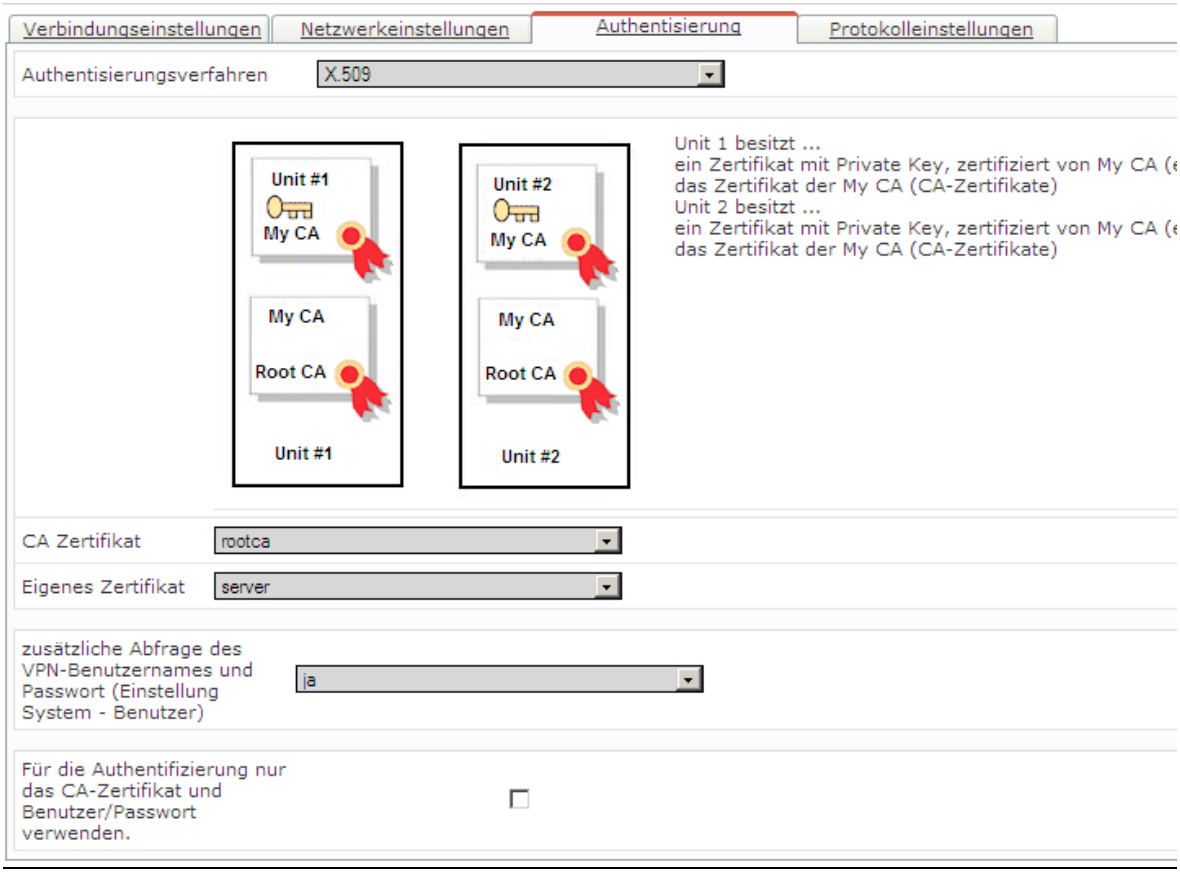


Abbildung 200

Registerkarte	Bezeichnung	Beschreibung
Authentisierung X.509 (Server)	**CA Zertifikat**	Dies ist das Stammzellenzertifikat(RootCA). Von diesem Zertifikat müssen alle anderen Zertifikate abstammen
	Eigenes Zertifikat	Mit diesem Zertifikat authentifizieren Sie sich gegenüber ihrem VPN-Partner
	Zusätzlich Abfrage des VPN-Benutzernamens und Passwort	Es ist möglich, dass zusätzlich noch Benutzerdaten von einwählenden Client gefordert werden. Bitte beachten Sie hierbei, dass diese Benutzerdaten im VPN-Server unter *System-Benutzer* eingetragen sein müssen
	Das eigene Zertifikat nicht für die Authentifizierung benutzen. Nur das CA Zertifikat und die Benutzerdaten verwenden	Mit dieser Option authentifizieren Sie sich nur über das CA-Zertifikat und die Benutzerdatenbank des VPN-Servers (Menü System-Benutzer)

18.2.3.3.4 Client

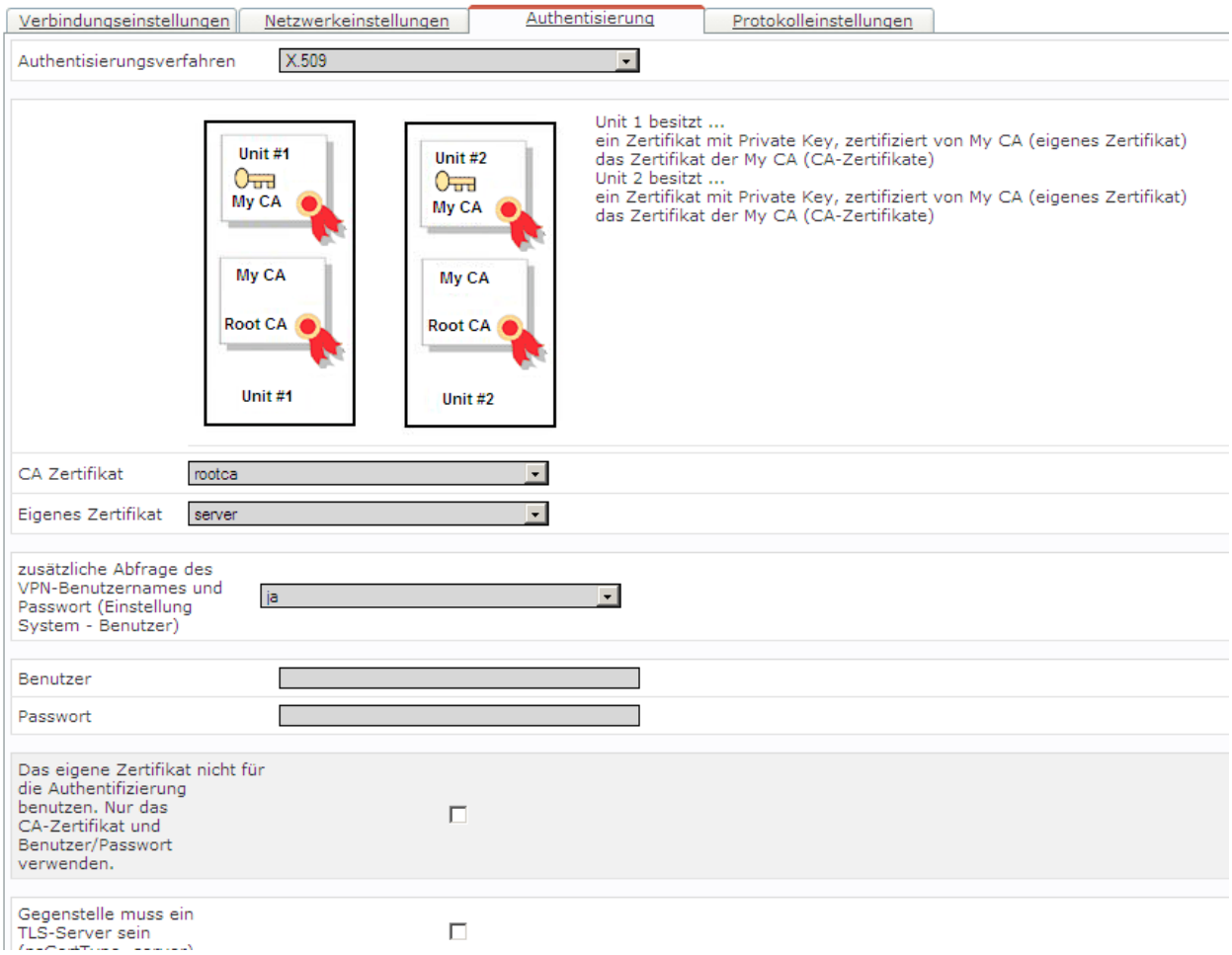


Abbildung 201

Registerkarte	Bezeichnung	Beschreibung
Authentisierung X.509 (Client)	**CA Zertifikat**	Dies ist das Stammzellenzertifikat(RootCA). Von diesem Zertifikat müssen alle anderen abstammen
	Eigenes Zertifikat	Mit diesem Zertifikat authentifizieren Sie sich gegenüber ihrem VPN-Partner
	Zusätzlich Abfrage des VPN-Benutzernamens und Passwort	Es ist möglich, dass zusätzlich noch Benutzerdaten von einwählenden Client gefordert werden. Bitte beachten Sie hierbei, dass diese Benutzerdaten im VPN-Server unter *System-Benutzer* eingetragen sein müssen
	Benutzerdaten	Tragen Sie hier die Benutzerdaten vom VPN-Server (aus System-Benutzer) ein
	Das eigene Zertifikat nicht für die Authentifizierung benutzen. Nur das CA Zertifikat und die Benutzerdaten verwenden	Mit dieser Option authentifizieren Sie sich nur über das CA-Zertifikat und die Benutzerdaten des VPN-Servers (aus System-Benutzer)
	Gegenstelle muss ein TLS-Server sein	Dies ist eine zusätzliche Sicherheitsoption. Das „Server-Zertifikat“ muss den Zusatz `nsCertType=server` unbedingt eingetragen haben (siehe Kapitel Erstellen von Zertifikaten).

18.3 Inaktivitätseinstellungen

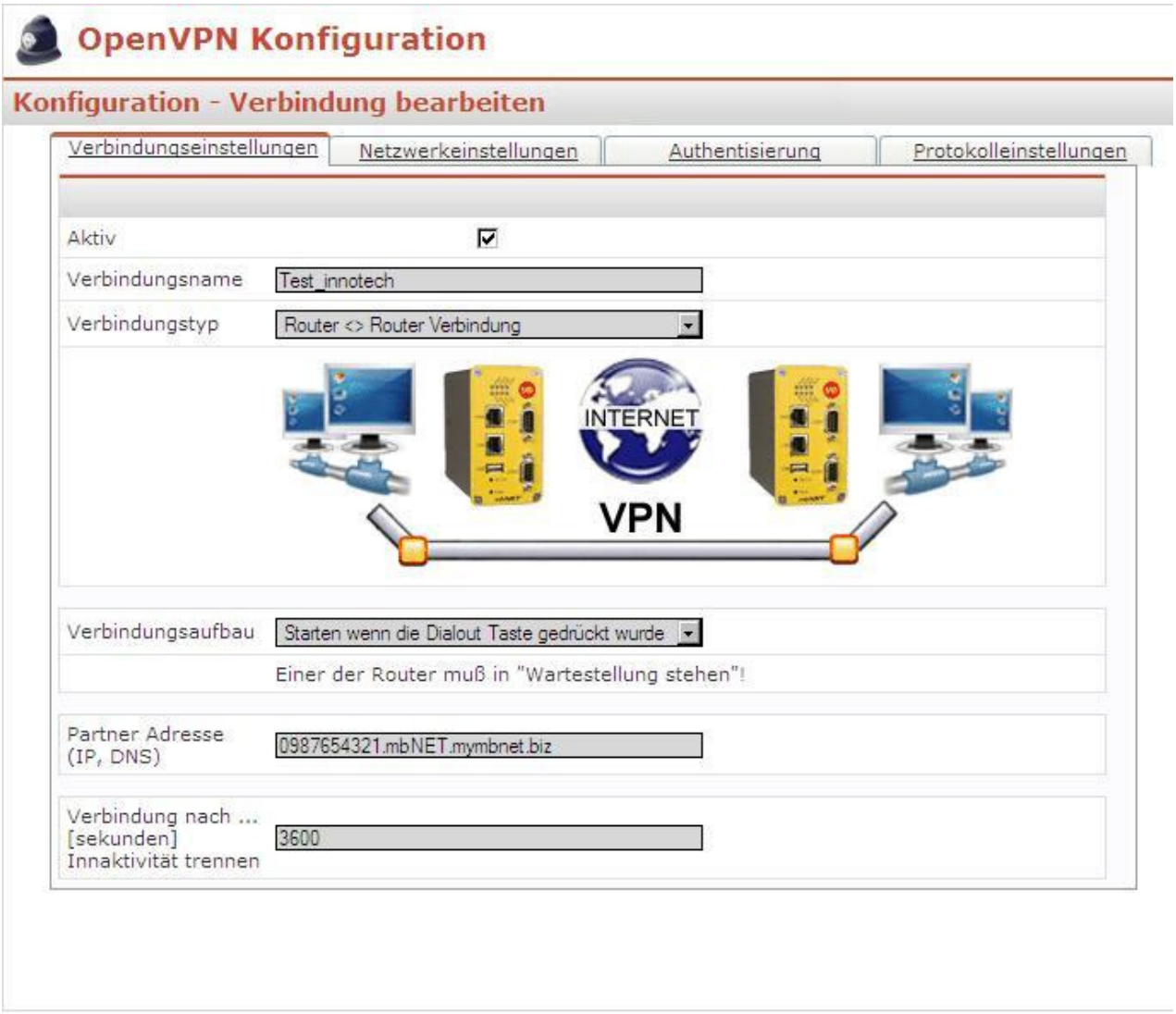


Abbildung 202

Sollte der OpenVPN-Verbindung über einen digitalen Eingang oder die Dialout-Taste gestartet werden, wird die Verbindung nach einer eingestellten Zeit - ohne Datenverkehr - selbstständig abgebaut.

18.4 Protokolleinstellungen

OpenVPN bietet eine Reihe von zusätzlichen Einstellmöglichkeiten. Eine beschriebene Übersicht ist auf der nächsten Seite aufgeführt.

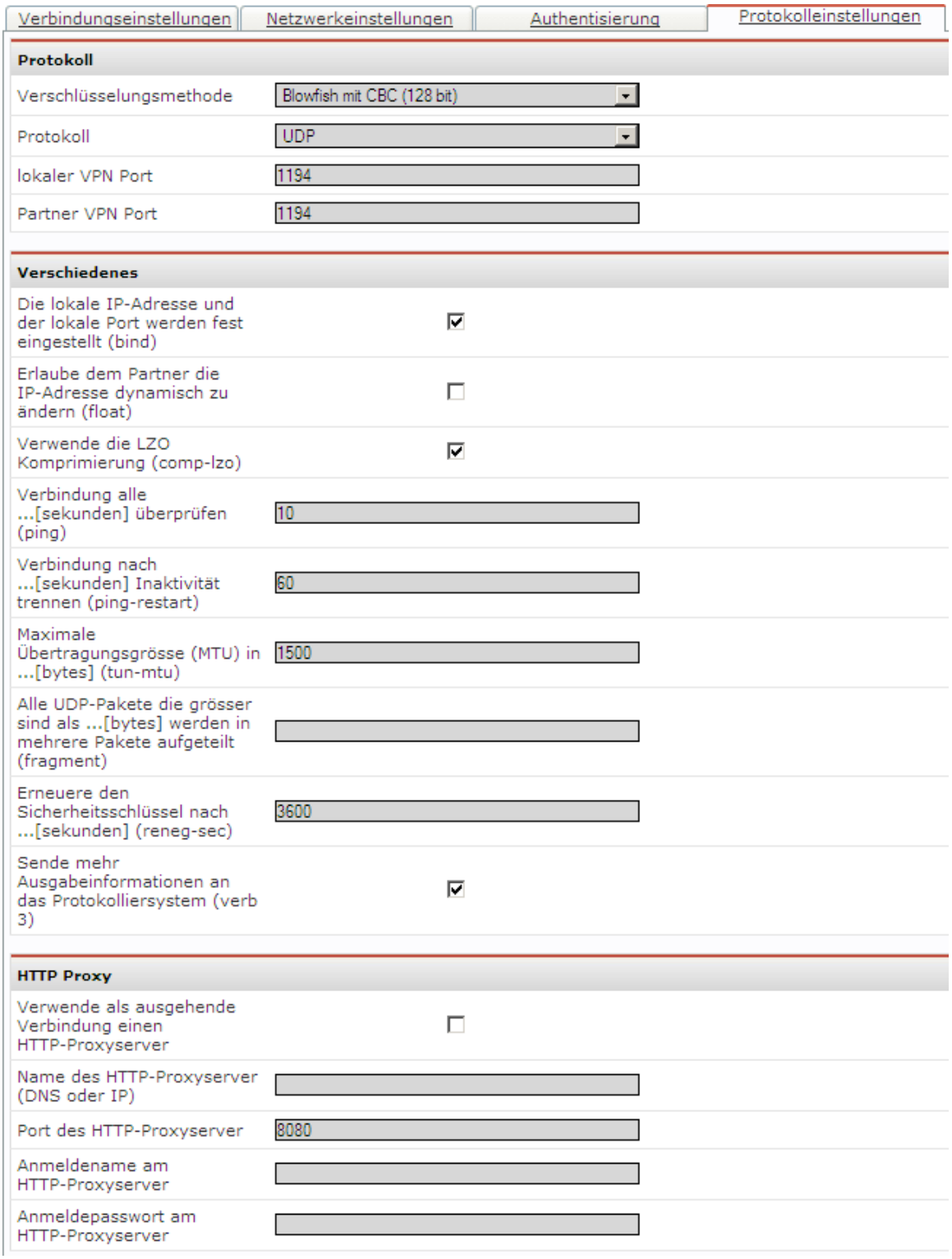
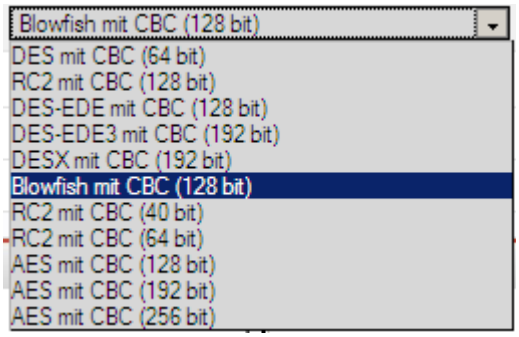


Abbildung 203

Registerkarte	Bezeichnung	Beschreibung
Protokoll-einstellungen	**Verschlüsselungs-Methode**	 **Abbildung 204** Diese Einstellung muss bei den Partnern gleich sein
	Protokoll	Es kann zwischen UDP und TCP gewählt werden. Die Standardeinstellung ist UDP. Wird der http-Proxy gewählt, gilt automatisch TCP
	Lokaler/Partner VPN-Port	Über die eingestellten Ports wird die OpenVPN Kommunikation geführt. In der Regel sind diese Ports gleich eingestellt. Standardmäßig ist es Port 1194
	Die lokale Adresse und der lokale Port werden fest eingestellt	OpenVPN kann die Ports nicht dynamisch während der Verbindung ändern.
	Erlaube dem Partner die Adresse dynamisch zu ändern	Mit dieser Option kann dem VPN-Partner erlaubt werden, seine IP-Adresse während der Verbindung zu ändern
	Verwende die LZO Komprimierung	Komprimierungsmethode von OpenVPN
	Verbindung alle n Sekunden überprüfen	Falls der OpenVPN-Tunnel n-Sekunden lang nicht in Benutzung war, wird ein ping an den VPN-Partner gesendet
	Verbindung nach n Sekunden Inaktivität trennen	Sollte der VPN-Partner nicht innerhalb von n-Sekunden auf den Ping antworten, oder kein Datenpaket empfangen, wird der Tunnel neu gestartet.
	Maximale Übertragungsgröße (MTU)	Standardgröße der MTU ist 1500 Byte
	Alle UDP-Pakete die größer sind als n Bytes werden gesplittet	Pakete die größer sind als n-Bytes werden aufgeteilt
	Erneuere den Sicherheitsschlüssel nach n Sekunden	Nach n-Sekunden wird ein neuer Schlüssel vereinbart. Standardmäßig ist dies auf 3600 Sekunden gesetzt.

	Sende mehr Ausgabe Informationen an das Protokollierungs-system	Dies entspricht der Einstellung „verb 3“ von OpenVPN. Default ist „aus“.
	Verwende als ausge-hende Verbindung einen http-Proxy	Wenn Sie ihre Verbindung zum Internet über einen HTTP-Proxy-Server aufbauen möchten, dann müssen Sie hier die Checkbox aktivieren
	Name des http-Proxy	Tragen Sie die IP oder den DNS-Namen des Proxy-Servers ein
	Port des http-Proxy	Bitte geben Sie hier den Port ein, über den ihr Proxy-Server die Anfragen entgegennimmt (Bsp. 8080 oder 3128)
	Anmeldedaten am http-Proxy	Sollte ihr Proxy-Server eine Authentifizierung verlan-gen, dann geben Sie einen gültigen Benutzernamen und das zugehörige Passwort ein.

19. Alarmmanagement

19.1 Allgemeines

Mit Hilfe des Alarmmanagements können

- die Zustände an den vier digitalen Eingängen abgefragt und in Abhängigkeit davon entsprechender Text an eine von Ihnen vorgegebene Emailadresse versendet werden.
- zwei digitale Ausgänge bei einer Gerätestörung bzw. bei einer aktiven Internetver-bindung oder manuell unabhängig voneinander geschaltet werden.

19.2 Digitale Eingänge

Klicken Sie in der Navigationsleiste auf den Menüpunkt **Alarmmanagement** und **Eingang**

Daraufhin wird die nachfolgende Bildschirm-maske zur Konfiguration der vier zur Verfü-gung stehenden digitalen Eingänge ange-zeigt. Über die vier verschiedenen Register-karten können die Eingänge einzeln konfigu-riert werden.

Abbildung 205

Alarmmanagement (Fortsetzung)

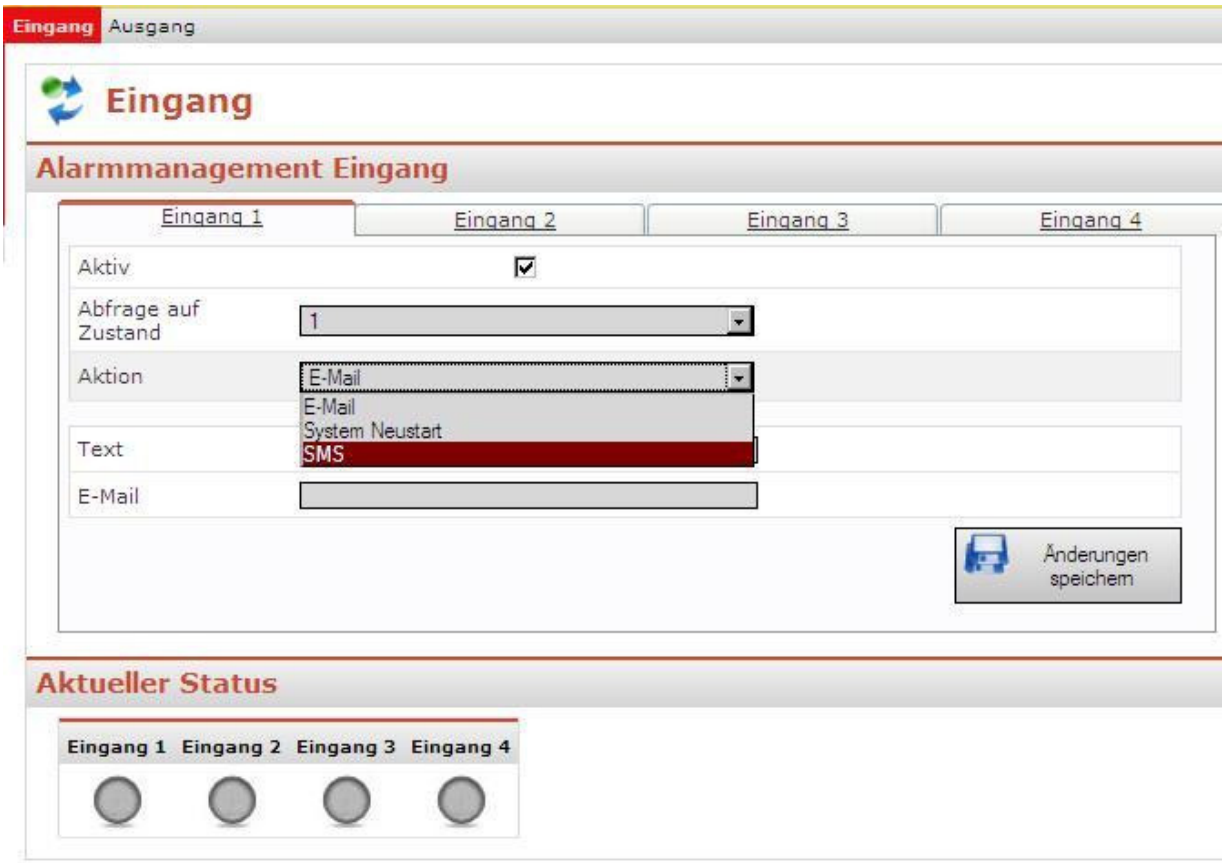


Abbildung 206

Bezeichnung	Funktion
Registerkarten Eingang 1 4	Jeder Eingang kann separat konfiguriert werden. Wählen Sie durch Anklicken der entsprechenden Registerkarte den zu konfigurierenden Eingang aus.
Aktiv	Der Eingang ist aktiviert, wenn Sie die Checkbox durch Anklicken mit einem Häkchen versehen. Wählen Sie hiermit aus, ob der entsprechende Eingang aktiviert („scharf geschaltet“) werden soll.
Abfrage auf Zustand	Stellen Sie mit diesem Auswahlfeld ein, auf welchen Eingangspegel der Industrierouter reagieren soll. Zur Auswahl stehen die Signalpegel 1 oder 0.
Aktion	Als Aktionen stehen 3 Möglichkeiten zur Verfügung: ☐ EMail versenden ☐ Kurznachricht versenden ☐ System Neustart
Text	Tragen Sie in diesem Eingabefeld ein, welcher Text mit der nachfolgend angegebenen Emailadresse versendet werden soll.
Emailadresse / Mobilgerätenummer	Geben Sie die EMailadresse bzw. die Telefonnummer ein, an die der Industrierouter den Text senden soll, wenn der Eingang aktiviert und der entsprechende Signalpegel zum Auslösen der Aktion geführt hat.
Aktueller Status	Über die symbolisch dargestellten Leuchtdioden am unteren Rand können Sie den momentanen Zustand an den Eingängen ablesen. Grau bedeutet Zustand 0, Grün bedeutet Zustand 1

19.3 Digitale Ausgänge

Klicken Sie in der Navigationsleiste auf den Menüpunkt **Alarmmanagement** und **Ausgang**

Daraufhin wird die nachfolgende Bildschirmmaske zur Konfiguration der zwei zur Verfügung stehenden digitalen Ausgänge angezeigt. Über die beiden Registerkarten können die Ausgänge separat konfiguriert werden.
Die Beschreibung sämtlicher Eingabe- und Auswahlfelder entnehmen Sie bitte den folgenden Seiten.

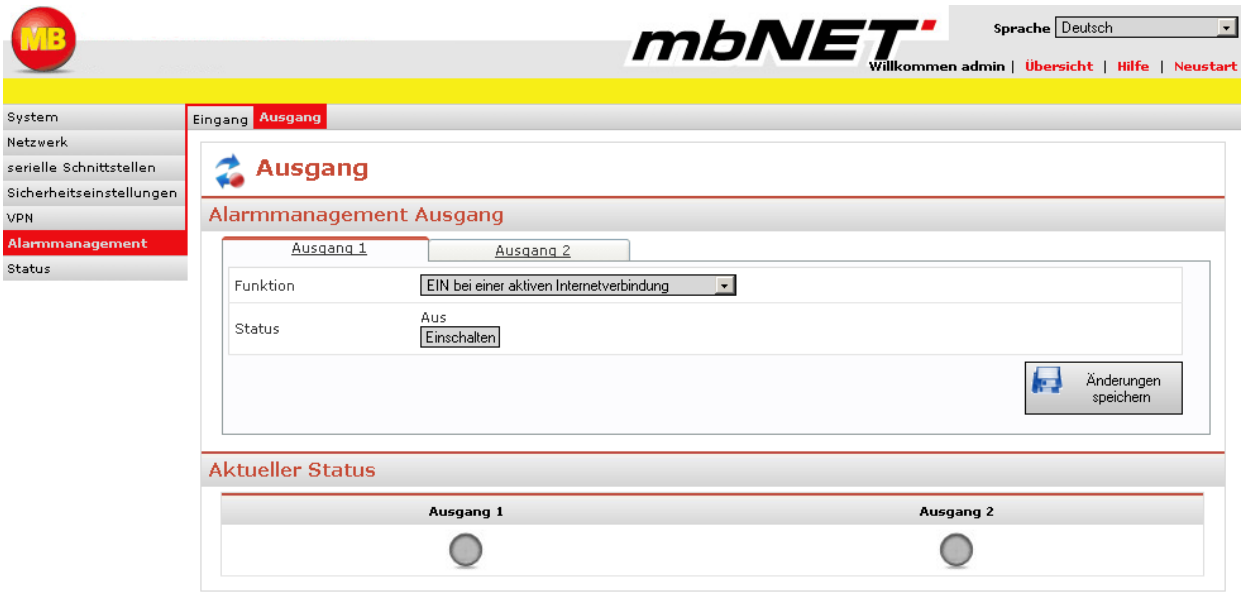


Abbildung 207

Bezeichnung	Funktion
Ausgang 1 **Ausgang 2**	Jeder Ausgang kann separat konfiguriert werden. Wählen Sie zur Konfiguration des entsprechenden Ausganges die entsprechende Registerkarte.
Funktion	Sie können über das Auswahlfeld unter folgenden Einstellungen auswählen: **Aus** Wählen Sie diese Einstellungen, wenn Sie die Ausgänge für evtl. Schaltvorgängen nicht auswerten möchten. **Ein bei einer Gerätestörung** Wählen Sie diese Einstellung, wenn der entsprechende Ausgang des Industrieroutes bei einer Gerätestörung auf Signalpegel 1 gesetzt werden soll. **Ein bei einer aktiven Internetverbindung** Wählen Sie diese Einstellung, wenn der entsprechende Ausgang des Industrieroutes bei einer Verbindung ins Internet auf 1 gesetzt werden soll. Zum Beispiel kann damit eine aktive Internetverbindung durch eine am Ausgang A1 oder A2 angeschlossene Leuchte signalisiert werden.
Status	**Einschalten** bzw. **Ausschalten** Über die Schaltfläche kann der momentan ausgewählte Ausgang ein- bzw. ausgeschaltet werden. Der Text **Aus** oder **An** über der Schaltfläche zeigt ebenso wie das LED-Symbol unter **Aktueller Status** den momentanen Zustand des Ausgangs an. **LED-Symbol grün:** Ausgang Signalpegel 1 **LED-Symbol grau:** Ausgang Signalpegel 0

20. Statusmeldungen

20.1 Allgemeines

Beim Auftreten von Fehlern ist der Industrierouter anhand bestimmter Statusinfos zu analysieren. So wird z.B. durch Blinken der ERROR-LED angezeigt, dass am Router ein Systemfehler aufgetreten ist. Hierzu kann z.B. über **Status** - **System** anhand der Auflistung evtl. festgestellt werden, wo die Fehlerursache liegt.
Nachfolgend die Beschreibung der verschiedenen Statusanzeigen:

20.2 Status - Schnittstellen

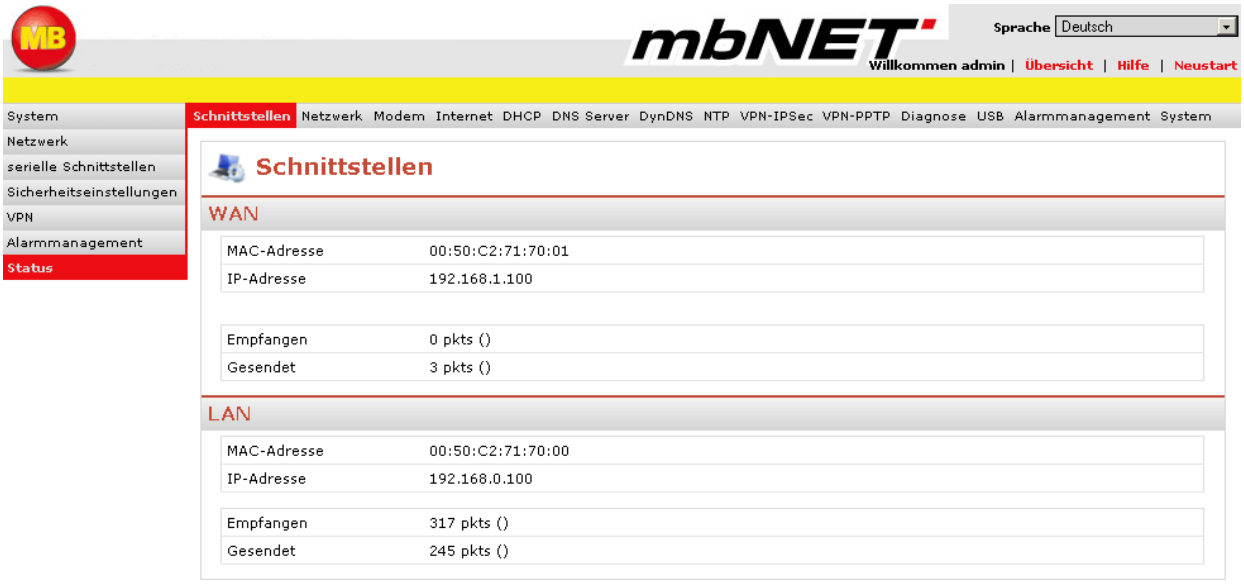


Abbildung 208

Bezeichnung	Funktion
WAN	Anzeige der Einstellungen am WAN-Anschluss (externer Anschluss) des Routers. Sobald der Router eine physikalische Verbindung zum Netzwerk hat, oder ihm eine statische IP-Adresse zugewiesen wird, dann wird die IP-Adresse angezeigt. Die Anzahl empfangener und gesendeter Datenpakete wird angezeigt.
LAN	Anzeige der Einstellungen am LAN-Anschluss (lokaler Anschluss) des Routers. Die IP-Adresse wird dann angezeigt, wenn der Router eine physikalische Verbindung hat. Die Anzahl empfangener und gesendeter Datenpakete wird angezeigt.

20.3 Status - Netzwerk

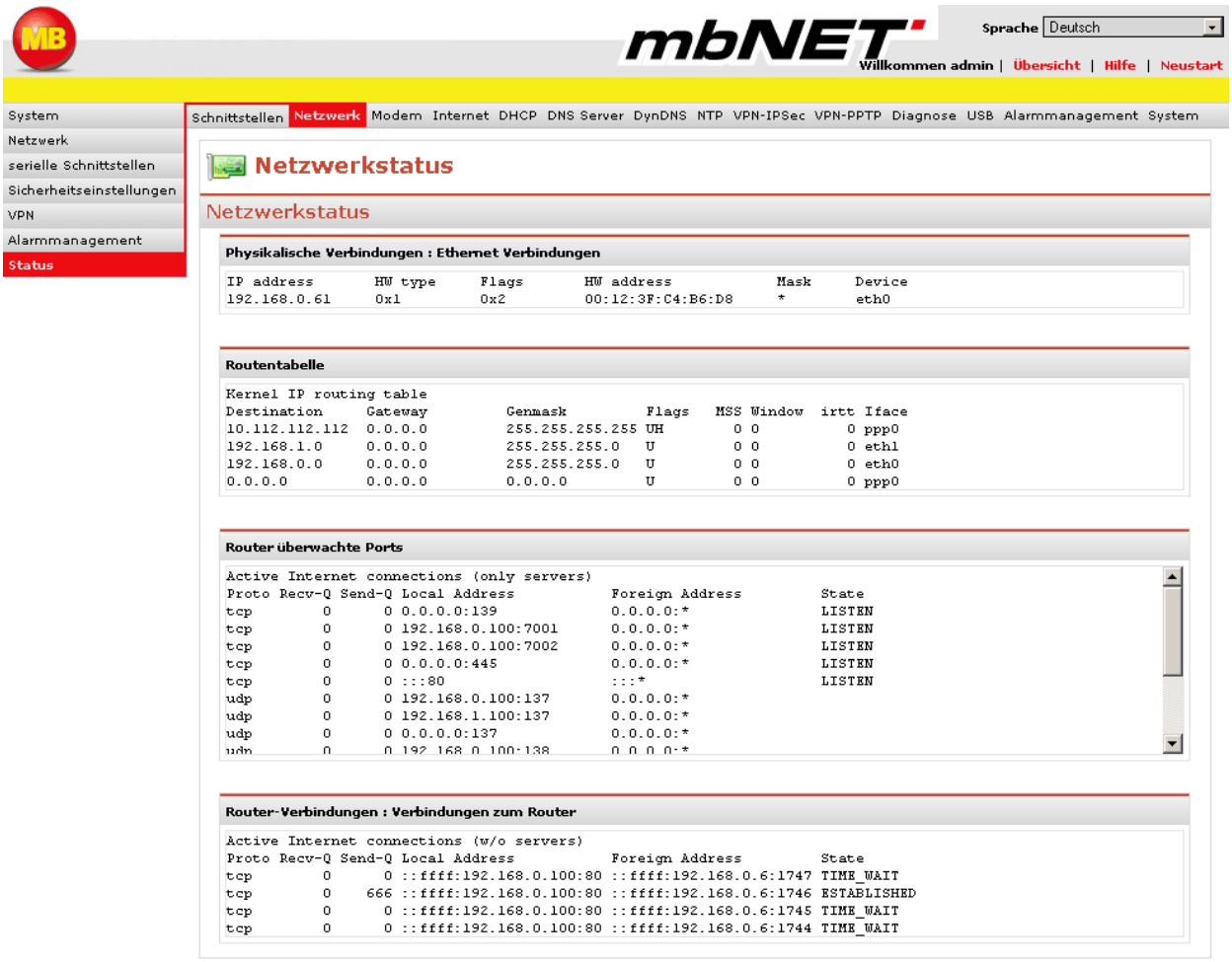

mbNET
Sprache Deutsch
Willkommen admin | Übersicht | Hilfe | Neustart
System
Netzwerk
serielle Schnittstellen
Sicherheitseinstellungen
VPN
Alarmmanagement
Status
Schnittstellen Netzwerk Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP Diagnose USB Alarmmanagement System
Netzwerkstatus
Netzwerkstatus
Physikalische Verbindungen : Ethernet Verbindungen
IP address HW type Flags HW address Mask Device
192.168.0.61 0x1 0x2 00:12:3F:C4:B6:D8 * eth0
Routentabelle
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
10.112.112.112 0.0.0.0 255.255.255.255 UH 0 0 0 ppp0
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
192.168.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
0.0.0.0 0.0.0.0 0.0.0.0 U 0 0 0 ppp0
Router überwachte Ports
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 0.0.0.0:139 0.0.0.0:* LISTEN
tcp 0 0 192.168.0.100:7001 0.0.0.0:* LISTEN
tcp 0 0 192.168.0.100:7002 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:445 0.0.0.0:* LISTEN
tcp 0 0 :::80 :::* LISTEN
udp 0 0 192.168.0.100:137 0.0.0.0:*
udp 0 0 192.168.1.100:137 0.0.0.0:*
udp 0 0 0.0.0.0:137 0.0.0.0:*
Router-Verbindungen : Verbindungen zum Router
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 ::ffff:192.168.0.100:80 ::ffff:192.168.0.6:1747 TIME_WAIT
tcp 0 666 ::ffff:192.168.0.100:80 ::ffff:192.168.0.6:1746 ESTABLISHED
tcp 0 0 ::ffff:192.168.0.100:80 ::ffff:192.168.0.6:1745 TIME_WAIT
tcp 0 0 ::ffff:192.168.0.100:80 ::ffff:192.168.0.6:1744 TIME_WAIT

Abbildung 209

Bezeichnung	Funktion
Physikalische Verbindungen	Zeigt die physikalischen Verbindungen über die der Router mit weiteren Rechnern verbunden ist.
Routentabelle	Zeigt alle Routen die verwendet werden.
Router überwachte Ports	Zeigt sämtliche überwachte Ports an.
Router-Verbindungen: Verbindungen zum Router	Zeigt sämtliche IP-Adressen mit Ports z.B. von Rechnern an, die mit dem Router verbunden sind.

20.4 Status - Modem

Abbildung 210

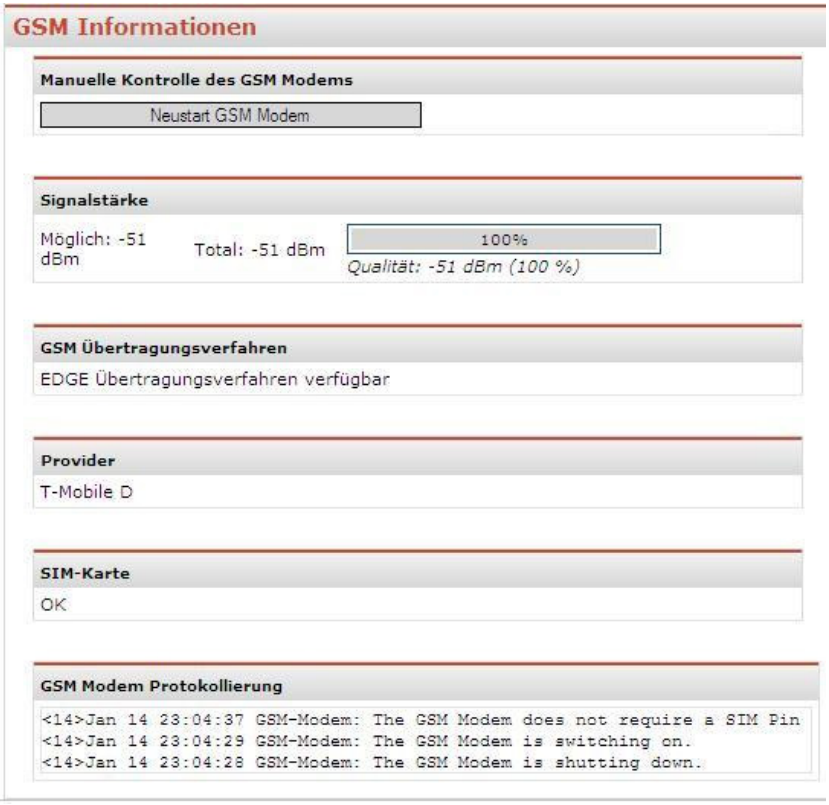


Abbildung 211

Bezeichnung	Funktion
Modem- verbindung	Es wird angezeigt welcher Benutzer sich per Modem auf den Router eingewählt hat. Bei erfolgreicher Wählverbindung werden IP-Adresse des PPP-Servers und des PPP-Clients (Gegenstelle) angezeigt. Hierbei handelt es sich immer um eingehende Verbindungen. Eine aktive Verbindung wird durch einen grün ausgefüllten Kreis symbolisiert.
Informationen der letzten Verbindung	Zeigt die Verbindungszeit und die Anzahl der gesendeten und empfangenen Bytes der letzten Verbindung an, solange der Router nicht neu gestartet oder zwischenzeitlich ausgeschaltet wurde.
Modem-kommando	Hiermit kann dem internen Modem direkt ein Befehl erteilt werden. **Benutzen Sie diese Funktion nur nach Anweisung des Supportpersonals von MB Connect Line!**
System Protokollierung	Zeigt Art der Verbindung und die vergebenen IP- und DNS-Adressen.
Modem Protokollierung	Es wird angezeigt, welche Befehle zur Initialisierung an das Modem geschickt werden und welchen Status der Verbindungsaufbau hat. Des Weiteren werden hier auch die Fehlermeldungen beim Verbindungsaufbau angezeigt.
Manuelle Kontrolle des GSM-Modems	Mit diesem Knopf können Sie das interne Modem neu starten. **Benutzen Sie diese Funktion nur nach Anweisung des Supportpersonals von MB Connect Line!**
Signalstärke	Hiermit wird die momentan Netzverfügbarkeit in Prozent und dBm angegeben. Wenn Sie ein mbNET mit Mobilfunk und UMTS besitzen, wird das Gerät automatisch die Netze wechseln wenn UMTS wieder verfügbar ist oder UMTS nicht mehr verfügbar ist.
GSM Übertrgungs-verfahren	Hier sehen Sie das jeweilige Übertragungsverfahren. Möglich sind: ☐ GSM/GPRS ☐ EDGE ☐ UMTS
Provider	Hier sehen Sie den momentanen Mobilfunkanbieter (T Mobile D wie in der Abbildung oben zu sehen)
SIM-Status	Hiermit wird der Status ihrer SIM-Karte im mbNET abgefragt
GSM-Modem protokollierung	Hier werden alle Ereignisse und Fehler des GSM-Modems eingetragen.

20.5 Status - Internet

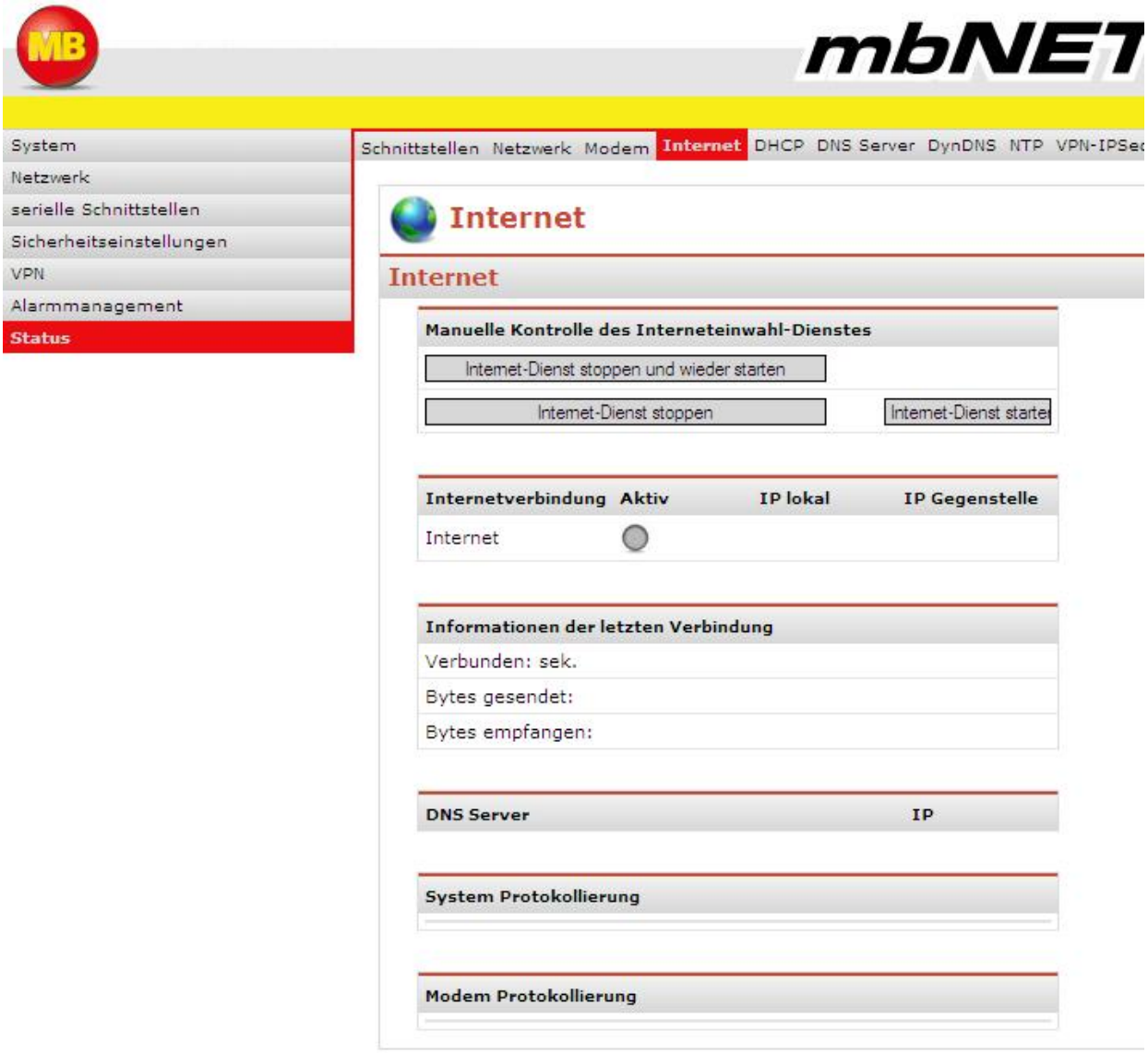


Abbildung 212

Bezeichnung	Funktion
Internet	Hierbei werden ausgehende Verbindungen ins Internet angezeigt. Dies können sowohl ausgehende Verbindungen über das Modem als auch Verbindungen über WAN sein. Es werden lokale und die IP-Adresse der Gegenstelle angezeigt. Eine aktive Verbindung wird durch einen grün ausgefüllten Kreis symbolisiert. Auch können Sie hier die Internetverbindung manuell trennen oder herstellen. **Es ist jedoch nicht empfohlen diese Knöpfe zu benutzen, außer Sie werden von einem Supportmitarbeiter dazu aufgefordert.**
Informationen der letzten Verbindung	Zeigt die Verbindungszeit und die Anzahl der gesendeten und empfangenen Bytes der letzten Verbindung an, solange der Router nicht neu gestartet oder zwischenzeitlich ausgeschaltet wurde.
DNS Server	Anzeige der IP-Adresse des DNS-Servers.
Systemprotokollierung	Zeigt Art der Verbindung und die vergebenen IP- und DNS-Adressen.
Modemprotokollierung	Es wird angezeigt, welche Befehle zur Initialisierung an das Modem geschickt werden und welchen Status der Verbindungsaufbau hat. Des Weiteren werden hier auch die Fehlermeldungen beim Verbindungsaufbau angezeigt.

20.6 Status - DHCP

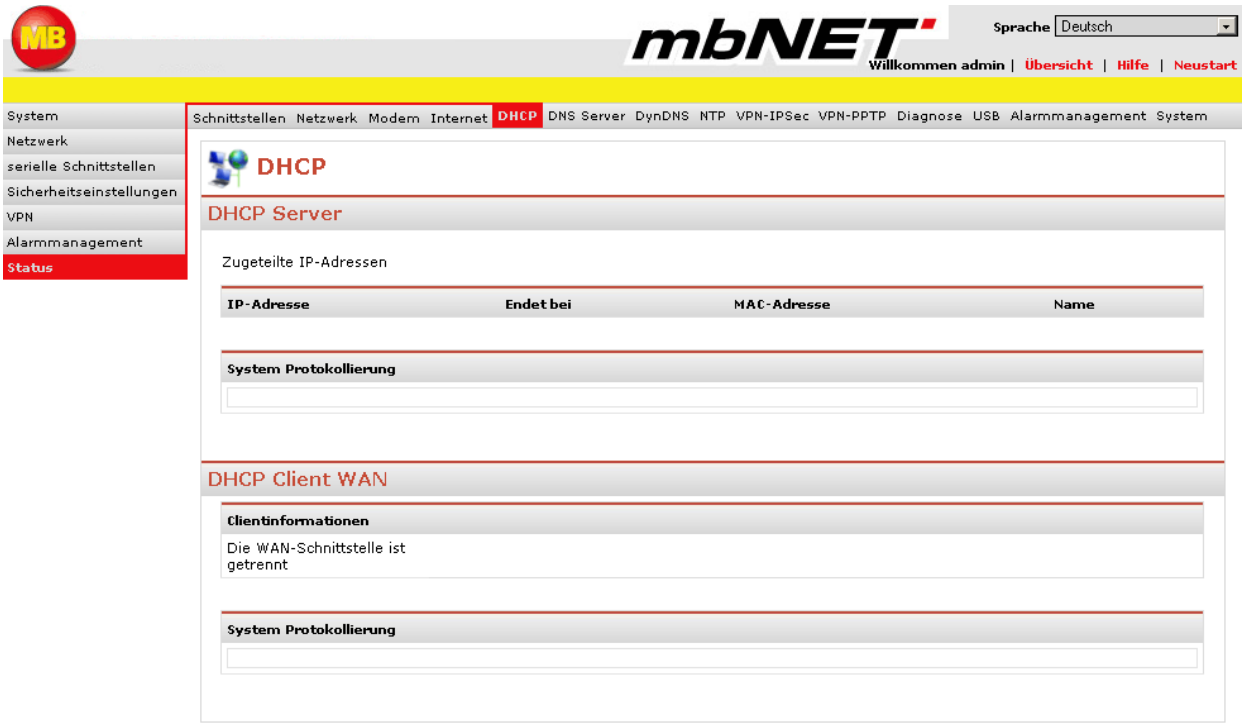


Abbildung 213

Bezeichnung	Funktion
DHCP-Server	Hier werden die IP-Adressen die der DHCP-Server an angeschlossene Clients vergibt, aufgelistet.
Systemproto-kollierung	Zeigt die IP-Adressen, die der DHCP vergibt und welche IP-Adressen unzulässig sind.
Client-informationen	Information über angeschlossene Clients am WAN-Anschluss.
Systemproto-kollierung	Hier werden alle Ereignisse und Fehler, die den DHCP-Server und -/Client betreffen.

20.7 Status - DNS-Server

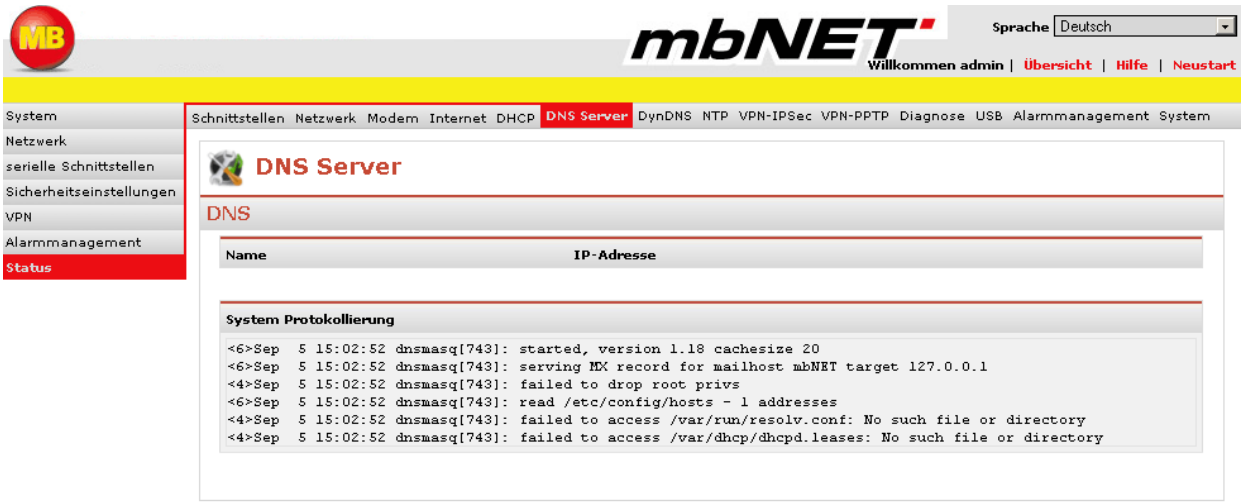

mbNET
Sprache Deutsch
Willkommen admin | Übersicht | Hilfe | Neustart
System
Netzwerk
serielle Schnittstellen
Sicherheitseinstellungen
VPN
Alarmmanagement
Status
Schnittstellen Netzwerk Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP Diagnose USB Alarmmanagement System
DNS Server
DNS
Name
IP-Adresse
System Protokollierung
<6>Sep 5 15:02:52 dnsmasq[743]: started, version 1.18 cachesize 20
<6>Sep 5 15:02:52 dnsmasq[743]: serving MX record for mailhost mbNET target 127.0.0.1
<4>Sep 5 15:02:52 dnsmasq[743]: failed to drop root privs
<6>Sep 5 15:02:52 dnsmasq[743]: read /etc/config/hosts - 1 addresses
<4>Sep 5 15:02:52 dnsmasq[743]: failed to access /var/run/resolv.conf: No such file or directory
<4>Sep 5 15:02:52 dnsmasq[743]: failed to access /var/dhcp/dhcpd.leases: No such file or directory

Abbildung 214

Bezeichnung	Funktion
Name	Anzeige des Namens von DNS-Server, falls nicht vom Internetserviceprovider vergeben.
IP-Adresse	Anzeige der IP-Adresse des DNS-Servers falls nicht vom Internetserviceprovider vergeben.
System Proto-kollierung	Anzeige der Arbeitsschritte, die der DNS Server ausführt.

20.8 Status - DynDNS

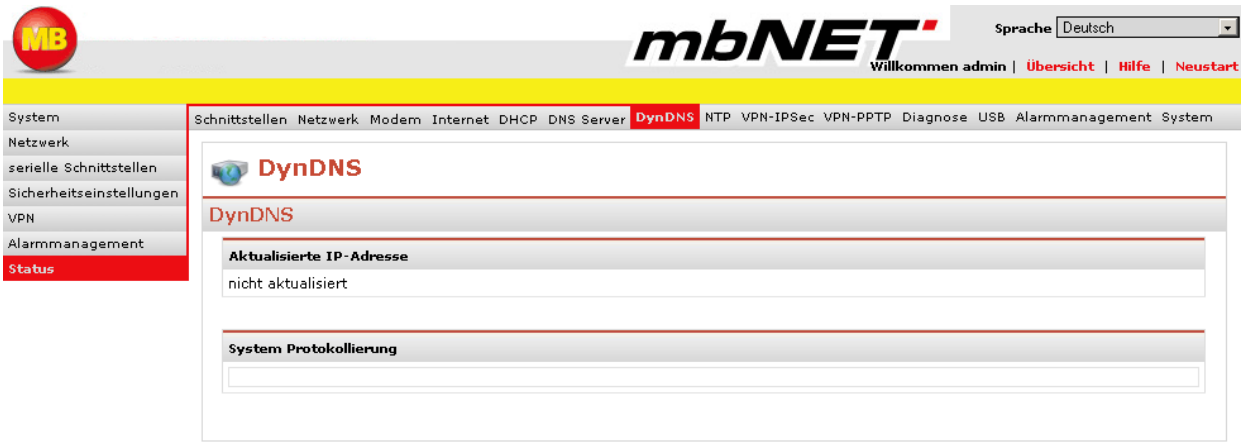


Abbildung 215

Bezeichnung	Funktion
Aktualisierte IP-Adresse	Anzeige der momentan aktuellen IP-Adresse die dem Router über das Internet zugewiesen wird.
Systemproto-kollierung	Hier werden alle Ereignisse und Fehler den DynDNS-Dienst betreffend angezeigt

20.9 Status - NTP

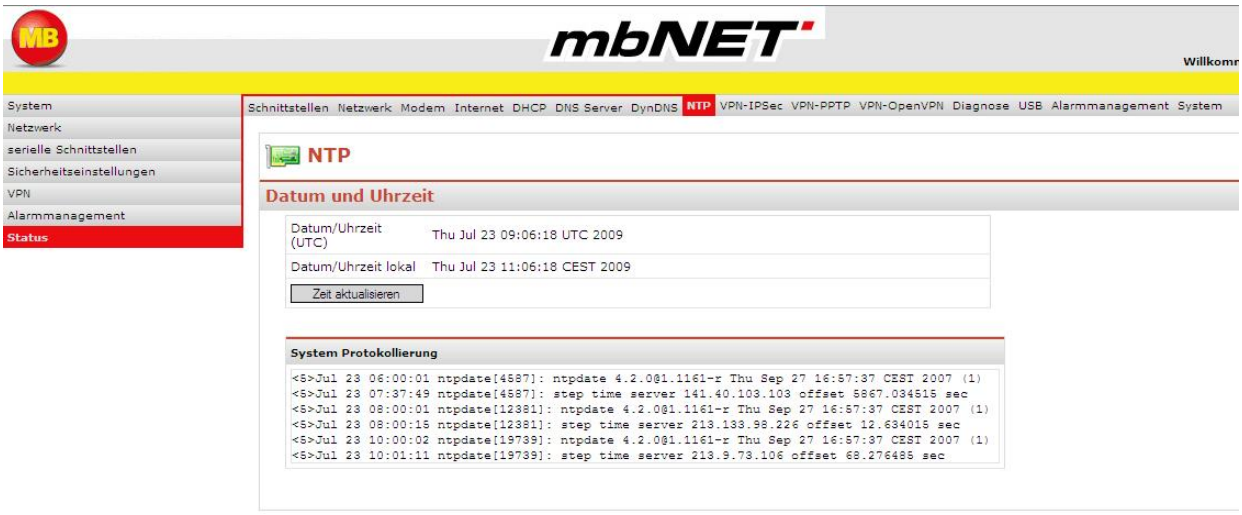

mbNET
System
Netzwerk
serielle Schnittstellen
Sicherheitseinstellungen
VPN
Alarmmanagement
Status
Schnittstellen Netzwerk Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP VPN-OpenVPN Diagnose USB Alarmmanagement System
NTP
Datum und Uhrzeit
Datum/Uhrzeit (UTC) Thu Jul 23 09:06:18 UTC 2009
Datum/Uhrzeit lokal Thu Jul 23 11:06:18 CEST 2009
Zeit aktualisieren
System Protokollierung
<5>Jul 23 06:00:01 ntpdate[4587]: ntpdate 4.2.0@1.1161-r Thu Sep 27 16:57:37 CEST 2007 (1)
<5>Jul 23 07:37:49 ntpdate[4587]: step time server 141.40.103.103 offset 5867.034515 sec
<5>Jul 23 08:00:01 ntpdate[12381]: ntpdate 4.2.0@1.1161-r Thu Sep 27 16:57:37 CEST 2007 (1)
<5>Jul 23 08:00:15 ntpdate[12381]: step time server 213.133.98.226 offset 12.634015 sec
<5>Jul 23 10:00:02 ntpdate[19739]: ntpdate 4.2.0@1.1161-r Thu Sep 27 16:57:37 CEST 2007 (1)
<5>Jul 23 10:01:11 ntpdate[19739]: step time server 213.9.73.106 offset 68.276485 sec

Abbildung 216

Bezeichnung	Funktion
Datum / Uhrzeit (UTC)	Anzeige der aktuellen Systemzeit in Universal Time Coordinates (UTC).
Datum / Uhrzeit lokal	Anzeige der Uhrzeit anhand der Einstellung der Zeitzone.
Systemproto-kollierung	Hier werden alle Benachrichtigungen und Fehlermeldungen des Dienstes ange-zeigt.

20.10 Status - VPN-IPSEC

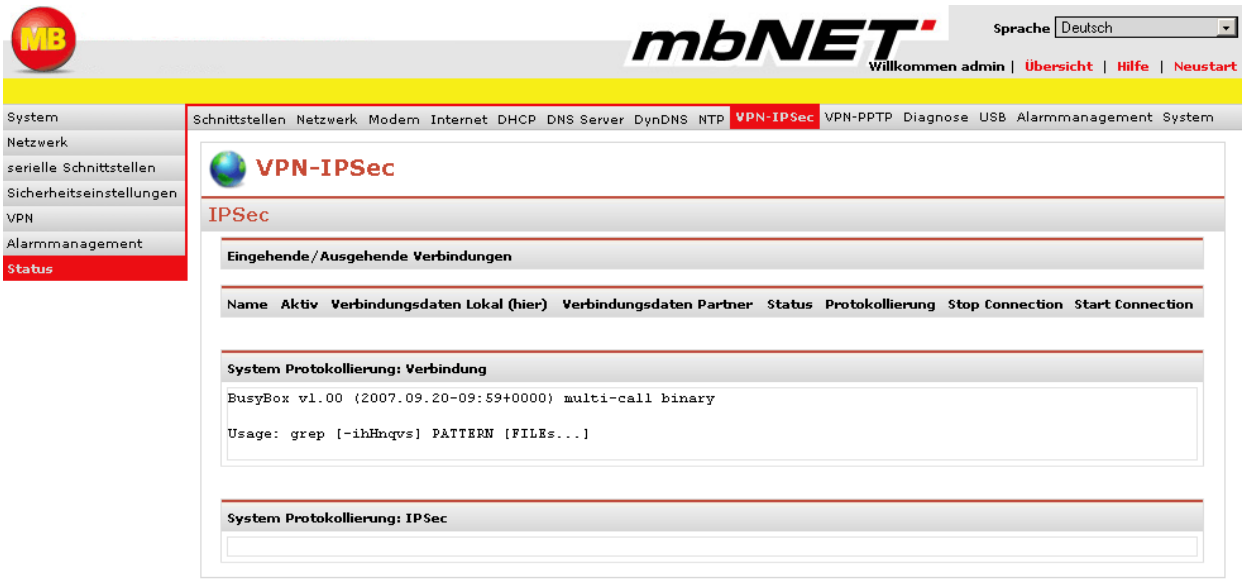
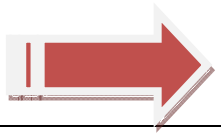


Abbildung 217

Bezeichnung	Funktion
Eingehende / Ausgehende Verbindungen 	Hier werden sowohl die eingehenden als auch die ausgehenden VPN-Verbindungen des Routers angezeigt. Eine aktive Verbindung wird durch einen grün ausgefüllten Kreis dargestellt. Die Verbindungsdauer und der eingewählte Benutzer werden angezeigt. Nach der Trennung der Verbindung wird die Zeit angezeigt, wie lange die entsprechende Verbindung aktiv war. Auch können Sie hier die Verbindung manuell trennen oder verbinden. **Es ist jedoch nicht empfohlen diese Knöpfe zu benutzen, außer Sie werden von einem Supportmitarbeiter dazu aufgefordert!**

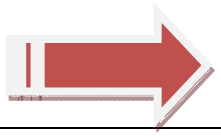
20.11 Status - VPN-PPTP

Abbildung 218

Bezeichnung	Funktion
Server	Hier werden die eingehenden VPN-Verbindungen des Routers aufgeführt. Eine aktive Verbindung wird durch einen grün ausgefüllten Kreis dargestellt. Es werden Verbindungsdauer, der eingewählte Benutzer, lokale und entfernte IP-Adresse angezeigt. Nach einer Trennung der Verbindung können Sie ablesen, wie lange die entsprechende Verbindung aktiv war.
Clients	Hier werden die vom Router ausgehenden VPN-Verbindungen angezeigt. Eine aktive Verbindung wird durch einen grün ausgefüllten Kreis dargestellt. Es werden Verbindungsdauer, der eingewählte Benutzer, lokale und entfernte IP-Adresse angezeigt. Die Verbindungen werden protokolliert. Nach einer Trennung der Verbindung können Sie ablesen, wie lange die entsprechende Verbindung aktiv war.
System Protokollierung: Verbindung	Hier werden alle Benachrichtigungen und Fehlermeldungen des PPTP-Dienstes angegeben.

20.12 Status – VPN OpenVPN

Abbildung 219

Bezeichnung	Funktion
Eingehende / Ausgehende Verbindungen 	Hier werden sowohl die eingehenden als auch die ausgehenden VPN-Verbindungen des Routers angezeigt. Eine aktive Verbindung wird durch einen grün ausgefüllten Kreis dargestellt. Name, Lokale und Partneradressen werden hier angezeigt. Auch können Sie hier manuell die Verbindung trennen oder aufbauen. **Es ist jedoch nicht empfohlen diese Knöpfe zu benutzen, außer Sie werden von einem Supportmitarbeiter dazu aufgefordert.**

20.13 Status - Diagnose

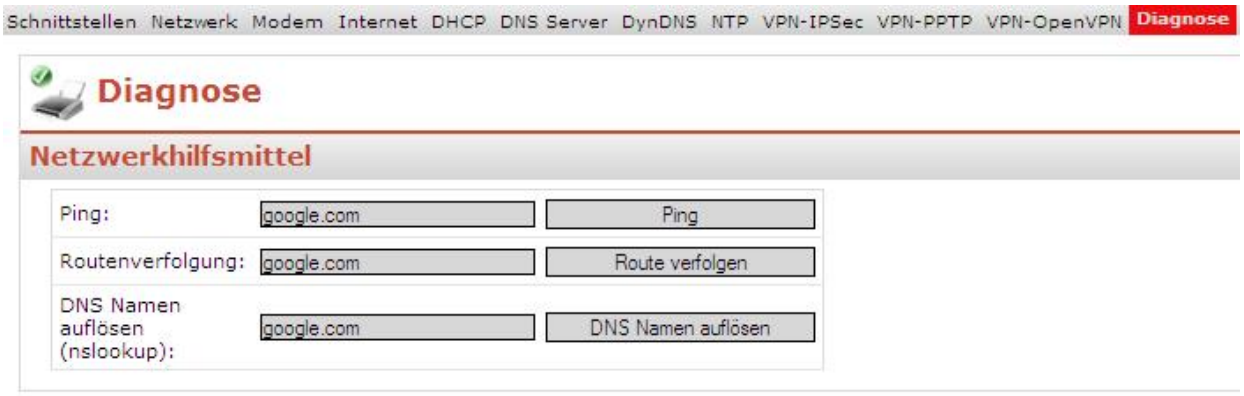


Abbildung 220

Bezeichnung	Funktion
Ping	Nach Eingabe einer Internetadresse oder einer IP-Adresse kann über den Ping-Befehl festgestellt werden, ob die entsprechende Adresse erreichbar ist. So kann z.B. u.a. leicht festgestellt werden ob eine Internetverbindung vorhanden ist.
Routenverfolgung	Mit diesem Befehl erhält man noch mehr Informationen über die Netzwerkverbindung zwischen Router und einem entfernten Rechner oder weiteren Router. Hier wird eine Routenverfolgung vorgenommen und sichtbar gemacht.
DNS-Namen auflösen	Mit dieser Funktion kann geprüft werden, ob eine Namensauflösung (http://www.mbconnectline.de = 88.12.12.34) stattfindet. Sollte diese Funktion in einer Fehlermeldung enden, dann prüfen Sie ob in ihrem mbNET eine DNS-Serveradresse unter *Netzwerk-DNS* eingetragen ist, oder ob der DNS-Server ihres Netzwerkes erreichbar ist.

20.14 Status - USB

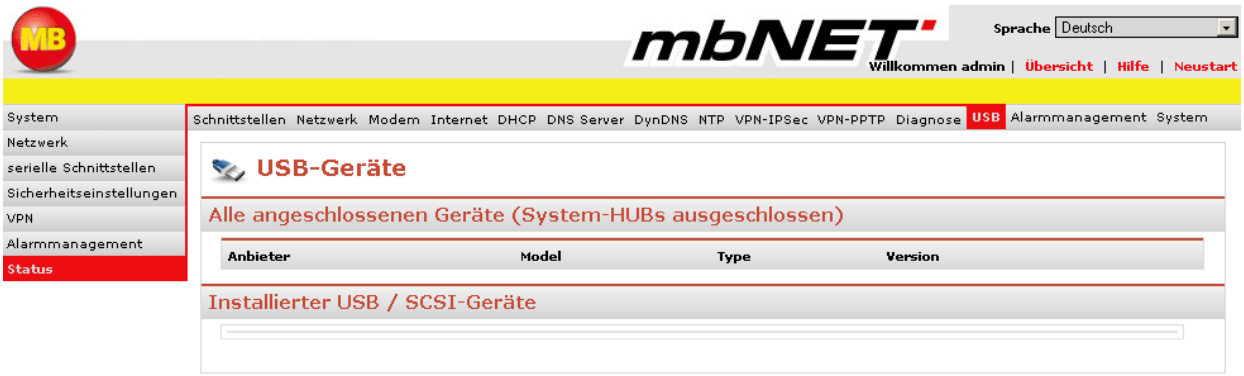


Abbildung 221

Bezeichnung	Funktion
Alle angeschlossenen Geräte (System-HUBs ausgeschlossen)	Bei angeschlossenem USB-Speicher, werden Anbieter, Modell, Typ und Version angezeigt.
Installierter USB / SCSI-Geräte	Darunter erfolgt eine Anzeige wie der USB-Speicher in das Dateisystem des Routers eingebunden ist und welches Dateisystem auf dem USB-Speicher angelegt ist.

20.15 Status - Alarmmanagement

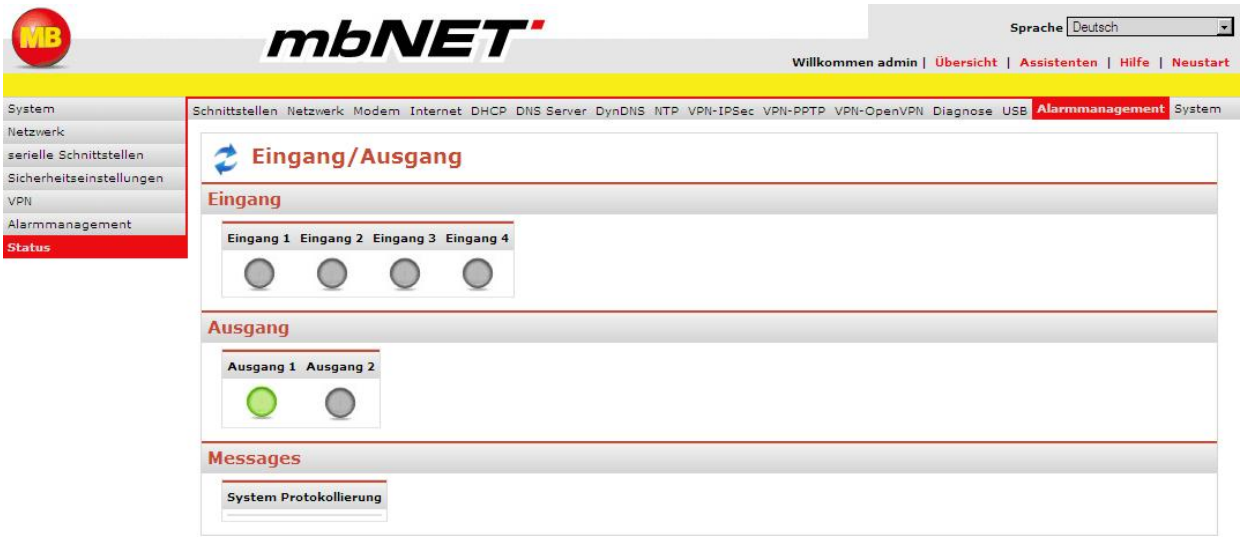


Abbildung 222

Bezeichnung	Funktion
Eingänge	Hier werden die Zustände an den Eingängen angezeigt. Die Abfrage der Zustände wird ca. alle drei Sekunden durchgeführt und aktualisiert.
Ausgänge	Hier werden die Zustände an den Ausgängen angezeigt. Die Abfrage der Zustände wird ca. alle drei Sekunden durchgeführt und aktualisiert.
Systemprotokollierung	Hier werden sämtliche Ereignisse und Fehlermeldungen gespeichert, die das Alarmmanagement betreffen (Bsp. Kurznachrichtenversand, Aktivität von Eingängen)

20.16 Status - System

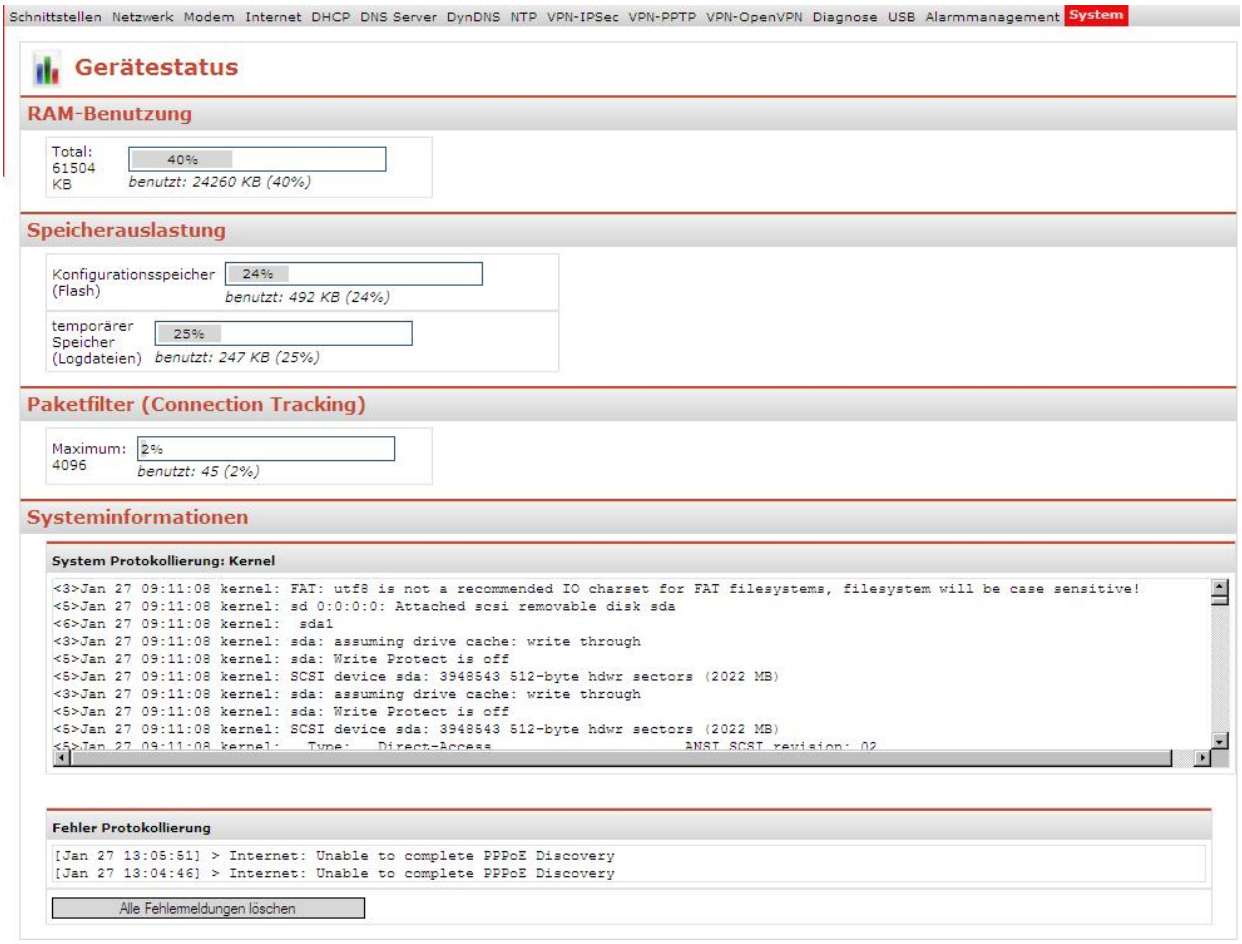

Schnittstellen Netzwerk Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP VPN-OpenVPN Diagnose USB Alarmmanagement System
Gerätestatus
RAM-Benutzung
Total: 61504 KB
40%
benutzt: 24260 KB (40%)
Speicherauslastung
Konfigurationsspeicher (Flash)
24%
benutzt: 492 KB (24%)
temporärer Speicher (Logdateien)
25%
benutzt: 247 KB (25%)
Paketfilter (Connection Tracking)
Maximum: 4096
2%
benutzt: 45 (2%)
Systeminformationen
System Protokollierung: Kernel
<3>Jan 27 09:11:08 kernel: FAT: utf8 is not a recommended IO charset for FAT filesystems, filesystem will be case sensitive!
<5>Jan 27 09:11:08 kernel: sd 0:0:0:0: Attached scsi removable disk sda
<6>Jan 27 09:11:08 kernel: sda1
<3>Jan 27 09:11:08 kernel: sda: assuming drive cache: write through
<5>Jan 27 09:11:08 kernel: sda: Write Protect is off
<5>Jan 27 09:11:08 kernel: SCSI device sda: 3948543 512-byte hdwr sectors (2022 MB)
<3>Jan 27 09:11:08 kernel: sda: assuming drive cache: write through
<5>Jan 27 09:11:08 kernel: sda: Write Protect is off
<5>Jan 27 09:11:08 kernel: SCSI device sda: 3948543 512-byte hdwr sectors (2022 MB)
Fehler Protokollierung
[Jan 27 13:05:51] > Internet: Unable to complete PPPoE Discovery
[Jan 27 13:04:46] > Internet: Unable to complete PPPoE Discovery
Alle Fehlermeldungen löschen

Abbildung 223

Bezeichnung	Funktion
RAM-Benutzung	Anzeige des momentan benötigten RAM-Speichers des Routers.
Speicherauslastung	Zeigt die Auslastung des Konfigurationsspeichers und des temporären Speichers.
Paketfilter	Zeigt die Auslastung des Paketfilters.
Systeminformationen	Über die Systeminformationen können evtl. Fehlerursachen am Router herausgefunden werden. Blinkt z.B. die ERROR-LED an der Frontseite, dann kann hier evtl. anhand der Protokollierung herausgefunden werden, wo die Fehlerursache liegt.
Fehlerprotokollierung	Seit der Firmware 2.1.0 gibt es eine direkte Fehlerprotokollierung in der Weboberfläche. Hier werden alle Fehler solange gespeichert, bis der Knopf „Alle Fehlermeldungen löschen“ gedrückt. Zusätzlich wird auf der Seite *System-Info* und der *Assistentsseite* der zuletzt aufgetretene Fehler angezeigt. Um von einer der beiden Seiten direkt zum Fehlerspeicher zu gelangen, muss nur auf die letzte Fehlermeldung gedrückt werden.

21. Werksseitige Einstellung bei Auslieferung

21.1 Benutzername und Passwort

Der Router wird mit folgendem angelegtem Benutzernamen und Passwort ausgeliefert:

Benutzername: admin

Passwort: kein Passwort notwendig

21.2 IP-Adresse des Routers

Der Router ist werksseitig auf folgende IP-Adresse eingestellt:

IP-Adresse: 192.168.0.100

22. Werkseinstellung laden

Befolgen Sie die unten aufgeführten Schritte um den Industrierouter wieder auf die Werkseinstellungen zurückzusetzen:

ACHTUNG: Sichern Sie **vorher** ihre Konfiguration. Nachdem diese Schritte unternommen wurden, sind alle von Ihnen vorgenommene Einstellungen nicht mehr vorhanden.

- ➔ Gerät einschalten
- ➔ Warten bis Ready-LED blinkt
- ➔ Dial Out Taste drücken und gedrückt halten bis TxD2 LED leuchtet
- ➔ Dial Out Taste erneut drücken (RxD2 leuchtet)
- ➔ Dial Out Taste nochmals drücken (TxD1 leuchtet)
- ➔ Zum Schluss ein letztes Mal Dial Out Taste drücken

Nun ist die individuell eingestellte Konfiguration gelöscht und der Industrierouter ist wieder in Werkseinstellung und kann neu konfiguriert werden.

ACHTUNG: Die IP-Adresse des Industrierouters wird auf 192.168.0.100 zurückgesetzt. Dementsprechend sind die Netzwerkeinstellungen des Rechners zu ändern.

23. Modeminitialisierung

Allgemeine Hinweise zu den AT-Befehlen

Die Befehle können in der Eingabeoberfläche (Modemeinstellungen) in die beiden Felder „Modem Initialisierung“ eingegeben werden.

Das **Präfix** besteht immer aus den Zeichen „**AT“.**
Dieser muss nicht in das Feld eingegeben werden.

Der **Befehl** setzt sich aus einzelnen Zeichen zusammen, die wie folgt beschrieben werden. Der Befehl besteht aus einem Kürzel und gegebenenfalls zugehörigen Werten.

Es wird Groß- und Kleinschreibung akzeptiert. Mehrere Befehle können zu einer Befehlszeile zusammengefasst werden.

Beispiel: L1M1\N5

23.1 Befehle des Analog-Modems

B **Kommunikationsstandard auswählen**

ATB0 CCITT Modulation
ATB1 Bell Modulation

\B **Behandlung des Break-Signals**

AT\Bn Break Signal zur Gegenstelle senden
n= 0-9 in 100 ms Einheiten (Standard AT\B3)
Nur bei nicht Fehlerkorrigierter Verbindung möglich

%C **Einstellung der Datenkompression**

AT%C0 Datenkompression inaktiv
AT%C1 Datenkompression aktiv

+GCI **Länderspezifische Einstellung**

Mit diesem Befehl wird das analoge Modem auf die länderspezifische Einstellung konfiguriert
Bsp. +GCI=B5

Modeminitialisierung (Fortsetzung)

L **Lautsprecher Lautstärke**

ATL0,1 geringe Lautstärke
ATL2 mittlere Lautstärke
ATL3 hohe Lautstärke

M **Lautsprecher Mode**

ATM0 Lautsprecher immer aus
ATM1 Lautsprecher ein, bis Datenträgersignal erkannt ist
ATM2 Lautsprecher ein, wenn das Modem wählbereit ist
ATM3 Lautsprecher aus, während die Rufnummer gewählt wird, dann nach dem Wählen ein, bis ein Datenträgersignal erkannt wird.

+MS **Modulationsart auswählen**

Mit diesem Kommando wird die Modulationsart und die Bit Raten, die zwischen dem lokalen und dem entfernten Modem ausgehandelt werden, eingestellt.
Syntax:
+MS=[<carrier>[,<automode>[,<min_tx_rate>[,<max_tx_rate>[,<min_rx_rate>[,<max_rx_rate>]]]]]

Beispiel: AT+MS= V34,1,9600,33600,9600,33600

Modulation	<carrier>	Mögliche Baudraten
Bell 103	B103	300
Bell 212	B212	1200 Rx 75 Tx oder 75 Rx/1200 Tx
V.21	V21	300
V.22	V22	1200
V.22 bis	V22B	1200, 2400
V.23	V23C	1200
V.32	V32	4800, 9600
V.32 bis	V32B	4800, 7200, 9600, 12000, 14400
V.34	V34	2400, 4800, 7200, 9600, 12000, 14400, 16800, 19200, 21600, 24000, 26400, 28800, 31200, 33600

Automode 0=deaktiviert
1=aktiviert (Standard)

AT+MS? Anzeige der aktuellen Einstellung

\N **Auswahl der Fehlerkorrektur**

AT\N0 Fehlerkorrektur ausgeschaltet
AT\N1 Transparente Übertragung beliebiger Datenbreiten über die serielle Schnittstelle, ohne Datenpufferung und Fehlerkorrektur.
AT\N2 V.42LAP-M oder MNP 4 Fehlerkorrektur. Kann keine fehlergesicherte Verbindung aufgebaut werden, legt das Modem auf.
AT\N3 V.42LAP-M oder MNP 4 Fehlerkorrektur. Kann keine fehlergesicherte Verbindung aufgebaut werden, wird eine nicht fehlergesicherte Verbindung angestrebt.
AT\N4 V.42LAP-M Fehlerkorrektur, ist dies nicht möglich legt das Modem auf.
AT\N5 MNP Fehlerkorrektur, ist dies nicht möglich legt das Modem auf.

Modeminitialisierung (Fortsetzung)

X Ausgabe der Meldungen, Wähltonerkennung

Dieses Kommando steuert, wie das Modem auf Wählton und Besetztsignal reagiert und wie es die CONNECT Meldungen anzeigt.

ATX0 Keine Besetzt- und Wähltonerkennung
d.h. bei einem erfolglosen Wählversuch wird NO CARRIER angezeigt.
Meldungen: OK, CONNECT, RING, NO CARRIER, ERROR und NO ANSWER werden angezeigt
ATX1 wie ATX0 aber CONNECTxxx Meldungen mit Geschwindigkeitsangabe
ATX2 Besetzttonerkennung deaktiviert, Wähltonerkennung aktiviert.
Meldungen: OK, CONNECT, RING, NO CARRIER, ERROR, NO ANSWER und NO DIAL TONE werden angezeigt
ATX3 Besetztton aktiviert, Wähltonerkennung deaktiviert.
Meldungen: OK, CONNECT xxx, RING, NO CARRIER, ERROR, NO ANSWER
ATX4 Besetztton und Wähltonerkennung aktiviert.
Meldungen: OK, CONNECTxxx, RING, NO CARRIER, ERROR, NO ANSWER und NO DIAL TONE

23.2 Befehle des ISDN Terminal Adapters (TA)

B Festlegung des Übertragungsprotokoll im B Kanal

ATB0: V.110 asynchron
ATB3: PPP asynchron zu synchron Konvertierung (PPP asynchron single link)
ATB4: HDLC transparent
ATB5: Byte transparent (B Kanal Daten)
ATB10: X.75 transparent
ATB13: V.120
ATB20: X.31 B Kanal (X.25 B Kanal)
ATB21: X.31 D Kanal

N Legt Übertragungsrate im V.110 Modus fest

ATN0 Verbindungsgeschwindigkeit automatisch
ATN1 Verbindungsgeschwindigkeit 1.200bit/s
ATN2 Verbindungsgeschwindigkeit 2.400bit/s
ATN3 Verbindungsgeschwindigkeit 4.800bit/s
ATN4 Verbindungsgeschwindigkeit 9.600bit/s
ATN5 Verbindungsgeschwindigkeit 19.200bit/s

#Z Definiert die MSN (multiple subscriber number)
Wird die Nummer auf „*“ (Stern) gesetzt (Standardeinstellung), wird jeder Anruf angenommen.
In der Regel muss aber eine MSN eingegeben werden, da dies die meisten TK-Anlagen verlangen. Außerdem muss die MSN für den Datendienst freigegeben werden.

AT#Z=n Setzt MSN auf n

24. Anhang

24.1 Ländercodes für analoge Geräte

Nr.	Land	Einstellung Modembetrieb
1	Afghanistan	B5
2	Albania(AL)	B5
3	Algeria(DZ)	B5
4	American Samoa(AS)	B5
5	Andorra(AD)	B5
6	Angola(AO)	B5
7	Anguilla(AI)	B5
8	Antarctica(AQ)	B5
9	Antigua and Barbuda(AG)	B5
10	Argentina(AR)	07
11	Armenia(AM)	B5
12	Aruba(AW)	B5
13	Australia(AU)	09
14	Austria(AT)	FD
15	Azerbaijan(AZ)	B5
16	Bahamas(BS)	B5
17	Bahrain(BH)	B5
18	Bangladesh(BD)	B5
19	Barbados(BB)	B5
20	Belarus(BY)	B5
21	Belgium(BE)	FD
22	Belize(BZ)	B5
23	Benin(BJ)	B5
24	Bermuda(BM)	B5
25	Bhutan(BT)	B5
26	Bolivia(BO)	B5
27	Bosnia and Herzegowina(BA)	B5
28	Botswana(BW)	B5
29	Bouvet Island(BV)	B5
30	Brazil(BR)	16
31	British Indian Ocean Territory(IO)	B5
32	Brunei Darussalam(BN)	B5
33	Bulgaria(BG)	FD
34	Burkina Faso(BF)	B5
35	Burundi(BI)	B5
36	Cambodia(KH)	B5
37	Cameroon(CM)	B5
38	Canada(CA)	B5
39	Cape Verde(CV)	B5
40	Cayman Islands(KY)	B5
41	Central African Republic(CF)	B5
42	Chad(TD)	B5
43	Chile(CL)	B5
44	China(CN)	B5
45	Christmas Island(CX)	B5

Nr.	Land	Einstellung Modembetrieb
46	Cocos (Keeling) Islands(CC)	B5
47	Colombia(CO)	B5
48	Comoros(KM)	B5
49	Congo(CG)	B5
50	Cook Islands(CK)	B5
51	Costa Rica(CR)	B5
52	Cote D'Ivoire(CI)	B5
53	Croatia(HR)	B5
54	Cuba(CU)	B5
55	Cyprus(CY),	FD
56	Czech Republic(CZ)	FD
57	Denmark(DK)	FD
58	Djibouti(DJ),	B5
59	Dominica(DM)	B5
60	Dominican Republic(DO)	B5
61	East Timor(TP)	B5
62	Ecuador(EC)	B5
63	Egypt(EG)	B5
64	El Salvador(SV)	B5
65	Equatorial Guinea(GQ)	B5
66	Eritrea(ER)	B5
67	Estonia(EE)	FD
68	Ethiopia(ET)	B5
69	Falkland Islands (Malvinas)(FK)	B5
70	Faroe Islands(FO)	B5
71	Fiji(FJ)	B5
72	Finland(FI)	FD
73	France(FR)	FD
74	France-Metropolitan(FX)	FD
75	French Guiana(GF)	B5
76	French Polynesia	B5
77	French Southern Territories(TF)	B5
78	Gabon(GA)	B5
79	Gambia(GM)	B5
80	Georgia(GE)	B5
81	Germany(DE)	FD
82	Ghana(GH)	B5
83	Gibraltar(GI)	B5
84	Greece(GR)	FD
85	Greenland(GL)	B5
86	Grenada(GD)	B5
87	Guadeloupe(GP)	B5
88	Guam(GU)	B5
89	Guatemala(GT)	B5
90	Guinea(GN)	B5
91	Guinea-Bissau(GW),	B5
92	Guyana(GY)	B5
93	Haiti(HT)	B5
94	Heard and Mc Donald Islands(HM)	B5

Nr.	Land	Einstellung Modembetrieb
95	Honduras(HN)	B5
96	Hong Kong(HK)	99
97	Hungary(HU)	FD
98	Iceland(IS)	FD
99	India(IN)	B5
100	Indonesia(ID)	99
101	Iran(Islamic Republic of)(IR)	B5
102	Iraq(IQ)	B5
103	Ireland(IE)	FD
104	Israel(IL)	B5
105	Italy(IT)	FD
106	Jamaica(JM)	B5
107	Japan(JP)	00
108	Jordan(JO)	B5
109	Kazakhstan(KZ)	B5
110	Kenya(KE)	B5
111	Kiribati(KI)	B5
112	Korea-Democratic People's Republic(KP)	B5
113	Korea-Republic of(KR)	B5
114	Kuwait(KW)	B5
115	Kyrgyzstan(KG)	B5
116	Lao People's Democratic Republic(LA)	B5
117	Latvia(LV)	FD
118	Lebanon(LB)	B5
119	Lesotho(LS)	B5
120	Liberia(LR)	B5
121	Libyan Arab Jamahiriya(LY)	B5
122	Liechtenstein(LI)	FD
123	Lithuania(LT)	FD
124	Luxembourg(LU)	FD
125	Macau(MO)	B5
126	Macedonia(MK)	B5
127	Madagascar(MG)	B5
128	Malawi(MW)	B5
129	Malaysia(MY)	6C
130	Maldives(MV)	B5
131	Mali(ML)	B5
132	Malta(MT)	FD
133	Marshall Islands(MH)	B5
134	Martinique(MQ)	B5
135	Mauritania(MR)	B5
136	Mauritius(MU)	B5
137	Mayotte(YT)	B5
138	Mexico(MX)	B5
139	Micronesia(Federated States of)(FM)	B5
140	Moldova-Republic of(MD)	B5
141	Monaco(MC)	B5
142	Mongolia(MN)	B5
143	Montserrat(MS)	B5

Nr.	Land	Einstellung Modembetrieb
144	Morocco(MA)	B5
145	Mozambique(MZ)	B5
146	Myanmar(MM)	B5
147	Namibia(NA)	B5
148	Nauru(NR)	B5
149	Nepal(NP)	B5
150	Netherlands(NL)	FD
151	Netherlands Antilles(AN)	FD
152	New Caledonia(NC)	B5
153	New Zealand(NZ)	7E
154	Nicaragua(NI)	B5
155	Niger(NE)	B5
156	Nigeria(NG)	B5
157	Niue(NU)	B5
158	Norfolk Island(NF)	B5
159	Northern Mariana Islands(MP)	B5
160	Norway(NO)	FD
161	Oman(OM)	B5
162	Pakistan(PK)	B5
163	Palau(PW)	B5
164	Panama(PA)	B5
165	Papua New Guinea(PG)	B5
166	Paraguay(PY)	B5
167	Peru(PE)	B5
168	Philippines(PH)	B5
169	Pitcairn(PN)	B5
170	Poland(PL)	FD
171	Portugal(PT)	FD
172	Puerto Rico(PR)	B5
173	Qatar(QA)	B5
174	Reunion(RE)	B5
175	Romania(RO)	FD
176	Russian Federation(RU)	B5
177	Rwanda(RW)	B5
178	St. Helena(SH)	B5
179	Saint Kitts and Nevis(KN)	B5
180	Saint Lucia(LC)	B5
181	St. Pierre and Miquelon(PM)	B5
182	Saint Vincent and the Grenadines(VC)	B5
183	Samoa(WS)	B5
184	San Marino(SM)	B5
185	Sao Tome and Principe(ST)	B5
186	Saudi Arabia(SA)	B5
187	Senegal(SN)	B5
188	Seychelles(SC)	B5
189	Sierra Leone(SL)	B5
190	Singapore(SG)	9C
191	Slovakia(SK)	FD
192	Slovenia(SI)	FD

Nr.	Land	Einstellung Modembetrieb
193	Solomon Islands(SB)	B5
194	Somalia(SO)	B5
195	South Africa(ZA)	9F
196	South Georgia, South Sandwich Islands(GS)	B5
197	Spain(ES)	FD
198	Sri Lanka(LK)	B5
199	Sudan(SD)	B5
200	Suriname(SR)	B5
201	Svalbard and Jan Mayen Islands(SJ)	B5
202	Swaziland(SZ)	B5
203	Sweden(SE)	FD
204	Switzerland(CH)	FD
205	Syrian Arab Republic(SY)	B5
206	Taiwan-Province of China(TW)	FE
207	Tajikistan(TJ)	B5
208	Tanzania-United Republic of(TZ)	B5
209	Thailand(TH)	B5
210	Togo(TG)	B5
211	Tokelau(TK)	B5
212	Tonga(TO)	B5
213	Trinidad and Tobago(TT)	B5
214	Tunisia(TN)	B5
215	Turkey(TR)	FD
216	Turkmenistan(TM)	B5
217	Turks and Caicos Islands(TC)	B5
218	Tuvalu(TV)	B5
219	Uganda(UG)	B5
220	Ukraine(UA)	B5
221	United Arab Emirates(AE)	B5
222	United Kingdom(UK)	FD
223	United States(US)	B5
224	United States Minor Outlying Islands(UM)	B5
225	Uruguay(UY)	B5
226	Uzbekistan(UZ)	B5
227	Vanuatu(VU)	B5
228	Vatican City State (Holy See)(VA)	B5
229	Venezuela(VE)	B5
230	Vietnam(VN)	99
231	Virgin Islands (British)(VG)	B5
232	Virgin Islands (U.S.)(VI)	B5
233	Wallis and Futuna Islands(WF)	B5
234	Western Sahara(EH)	B5
235	Yemen(YE)	B5
236	Yugoslavia(YU)	B5
237	Zaire(ZR)	B5
238	Zambia(ZW)	B5
239	Zimbabwe(ZW)	B5

25. Index

A

Alarmmanagement 170
Anzeige-, Bedienelemente und Anschlüsse 12
Auslieferungspasswort 21

B

Belegung 15
Benutzername und Passwort 190
Benutzername: 190

D

Digitale Ausgänge 172

E

Einstellungen speichern 27
Erste Konfiguration 21

F

Felder 23
Firewall 130
Forwarding 133

G

Grundkonfiguration 24

I

Inbetriebnahme des Routers 17

K

Kurzbeschreibung 8

L

LAN>WAN 132
Leistungsmerkmale 8
Lieferumfang 11

M

Modeminitialisierung 191

N

NAT 134
Netzwerk – Hosts 122
Netzwerk – Internet 118
Netzwerk – LAN 110
Netzwerk – Modem 113
Netzwerk – WAN 111
Netzwerk –DHCP 120
Netzwerk –DNS-Server 121
Netzwerk-DynDNS 123

P

Passwort 190

R

Rechneradresse (IP-Adresse) und Netzmaske einstellen 20

S

Schaltflächen 23
Schnittstellen 15
Schutzleiter 17
Serielle Schnittstellen 126
Serielle Schnittstellen auf Ihrem PC umleiten 129
Sicherheitseinstellungen 26, 130, 131, 134
Sicherheitshinweise 9
Startseite 22
Status - USB 187
Status-Alarmmanagement 188
Status-DHCP 179
Status-Diagnose 185, 186
Status-DNS-Server 180
Status-DynDNS 181
Status-Internet 177
Statusmeldungen (Auszug) 173
Status-Modem 175
Status-Netzwerk 174
Status-NTP 182
Status-Schnittstellen 173
Status-System 189
Status-VPN-IPSEC 183
Status-VPN-PPTP 184
Symbole 23
System - Firmware 108
System - Konfiguration 107
System - Protokollierung 106
System - USB 105
System - Zertifikate 99, 100, 102, 103, 104
Systemeinstellungen 24
System-WEB 95

T

Technische Daten 10

V

Verbindungsstatus 39
Verbindungsszenarien 28
VPN-Verbindung 60

W

WAN>LAN 131
Weboberfläche 22
Werksseitige Einstellung bei Auslieferung 190